$x^{2^l+1} + x + a$ and Related Affine Polynomials over GF(2^k)[☆]

Tor Helleseth, Alexander Kholosha

The Selmer Center, Department of Informatics, University of Bergen, PB 7800, N-5020 Bergen, Norway

Abstract

In this paper, the polynomials $P_a(x) = x^{2^l+1} + x + a$ with $a \in \mathrm{GF}(2^k)$ are studied. New criteria for the number of zeros of $P_a(x)$ in $\mathrm{GF}(2^k)$ are proved. In particular, a criterion for $P_a(x)$ to have exactly one zero in $\mathrm{GF}(2^k)$ when $\gcd(l, k) = 1$ is formulated in terms of the values of permutation polynomials introduced by Dobbertin. We also study the affine polynomial $a^{2^l}x^{2^{2l}} + x^{2^l} + ax + 1$ which is closely related to $P_a(x)$. In many cases, explicit expressions for calculating zeros of these polynomials are provided.

Key words: Equation over finite field, linearized polynomial, permutation polynomial, root.

1. Introduction

Denote $\mathrm{GF}(2^k)$ a finite field with 2^k elements, let $\mathrm{GF}(2^k)^* = \mathrm{GF}(2^k) \setminus \{0\}$ and $\mathrm{GF}(2^k)^{**} = \mathrm{GF}(2^k) \setminus \{0, 1\}$. Take positive integers k and l with $l < k$. The focus of this paper are the following polynomials over $\mathrm{GF}(2^k)$:

$$P_a(x) = x^{2^l+1} + x + a$$

with $a \in \mathrm{GF}(2^k)^*$. It is clear that $P_a(x)$ does not have multiple roots. These polynomials have recently arisen in several different contexts that include final geometry, constructing families of difference sets with Singer parameters

[☆]Research supported by the Norwegian Research Council.

Email addresses: Tor.Helleseth@uib.no (Tor Helleseth), Alexander.Kholosha@uib.no (Alexander Kholosha)

[1] and finding crosscorrelation between m-sequences [2, 3, 4]. First, we consider a particular case when l is coprime to k (which leads to an interesting new technique based on the use of Dobbertin polynomials) and then we take a general case with $\gcd(l,k) \geq 1$. With our results, we are able to distinguish between the case when $P_a(x)$ has none and the case when it has two zeros in $\mathrm{GF}(2^k)$ if $\gcd(l,k) > 1$. This is considered to be a hard problem in general. Finally, we study the roots of the following affine polynomial which is shown to be closely related to $P_a(x)$

$$F_a(x) = a^{2^l} x^{2^{2l}} + x^{2^l} + ax + 1 \ . \tag{1}$$

Polynomials $f(x) = x^{p^l+1} + ax + b$ over a field of characteristic p with an arbitrary l were recently extensively studied by Bluher in her paper [5]. Thus, here we consider a particular instance of this problem. However, as a main result of the paper, we prove new criteria for the number of zeros of $P_a(x)$ in $\mathrm{GF}(2^k)$. For instance, if $\gcd(l,k) = 1$ then the absolute trace of the particular value of the Dobbertin permutation polynomial defines whether $P_a(x)$ has a unique zero or not. We also give explicit polynomial formulas for calculating zeros in case when zero is unique or there are exactly two of them and k is odd. Note that $f(x)$ can always be transformed into the form $x^{p^l+1} + x + c$ by a simple substitution of variable x with sx having $s^{p^l} = a$ (such an $s \in \mathrm{GF}(p^k)$ always exists). Moreover, even a more general polynomial form $x^{p^l+1} + ax^{p^l} + bx + c$ can be reduced to $f(x)$ by setting x equal to $x - a$.

In the particular case when $l = 1$, the equation $P_a(x) = 0$ takes on the form $D_3(x) = a$ where $D_3(x) = x^3 + x$ is the third Dickson polynomial (a comprehensive reference on this topic is [6]). Denote

$$\mathcal{H}_i = \{x \in \mathrm{GF}(2^k)^* \mid \mathrm{Tr}_k(x^{-1}) = i\} \quad \text{for} \quad i = 0, 1$$

$r_0 = \gcd(3, 2^k - 1)$ and $r_1 = \gcd(3, 2^k + 1)$. Obviously, $r_0 = 1$ and $r_1 = 3$ (resp. $r_0 = 3$ and $r_1 = 1$) for k odd (resp. k even). From the well-known fact (see [6], [7, Proposition 5] or [2, Lemma 18]) if follows that $D_3(x)$ is a r_0-to-1 mapping of $\mathcal{H}_0 \setminus \{1\}$ into $\mathcal{H}_0$ and is a r_1-to-1 mapping of $\mathcal{H}_1 \setminus \{1\}$ into $\mathcal{H}_1$. Therefore, for odd k (resp. even k) $D_3(x) = a$ has a unique solution in $\mathrm{GF}(2^k)$ if and only if $a \in \mathcal{H}_0$ (resp. $a \in \mathcal{H}_1$) which for any k is equivalent to $\mathrm{Tr}_k(a^{-1} + 1) = 1$. In the other cases this equation can have either none or three solutions.

By the time the earlier version of this paper [8] was published, we where able to prove many relevant results assuming additional restrictive conditions. In the current paper, just Section 3 almost has not been changed compared to [8]. Sections 2 and 4 had been considerably revised to contain the results under the the most general conditions, some proof were rewritten in a simpler way. Sections 5 and 6 are completely new. We believe that a paper containing patches to [8] would be extremely reader-unfriendly since we would have to refer not just to the previous results but to the parts of the proofs in [8]. That is why we decided to submit a self-contained paper that does not require any prior reading.

2. Preliminaries

The finite field $\mathrm{GF}(2^d)$ is a subfield of $\mathrm{GF}(2^k)$ if and only if d divides k. The trace and norm mappings from $\mathrm{GF}(2^k)$ to the subfield $\mathrm{GF}(2^d)$ are defined respectively by

$$\mathrm{Tr}_d^k(x) = \sum_{i=0}^{k/d-1} x^{2^{id}} \qquad \text{and} \qquad \mathrm{N}_d^k(x) = \prod_{i=0}^{k/d-1} x^{2^{id}} \ .$$

In the case when $d = 1$, we use the notation $\mathrm{Tr}_k(x)$ instead of $\mathrm{Tr}_1^k(x)$. In this paper, also let M_i denote the number of $a \in \mathrm{GF}(2^k)^*$ such that $P_a(x)$ has exactly i zeros in $\mathrm{GF}(2^k)$.

If l is coprime to k, denote $l' = l^{-1} \pmod k$ and recall the following sequences of polynomials that were introduced by Dobbertin in [9] (see also [7]):

$$\begin{aligned}
A_1(x) &= x\,, \\
A_2(x) &= x^{2^l+1}\,, \\
A_{i+2}(x) &= x^{2^{(i+1)l}} A_{i+1}(x) + x^{2^{(i+1)l}-2^{il}} A_i(x) \quad \text{for} \quad i \geq 1\,, \\
B_1(x) &= 0\,, \\
B_2(x) &= x^{2^l-1}\,, \\
B_{i+2}(x) &= x^{2^{(i+1)l}} B_{i+1}(x) + x^{2^{(i+1)l}-2^{il}} B_i(x) \quad \text{for} \quad i \geq 1 \ .
\end{aligned}$$

These are used to define the polynomial

$$R(x) = \sum_{i=1}^{l'} A_i(x) + B_{l'}(x) \ . \tag{2}$$

As noted in [9], the exponents occurring in $A_j(x)$ (resp. in $B_j(x)$) are precisely those of the form

$$e = \sum_{i=0}^{j-1} (-1)^{\epsilon_i} 2^{il}$$

where $\epsilon_i \in \{0,1\}$ satisfy $\epsilon_{j-1} = 0$, $\epsilon_0 = 0$ (resp. $\epsilon_0 = 1$), and $(\epsilon_i, \epsilon_{i-1}) \neq (1,1)$.

Further, we will essentially need the following result proven in [9, Theorem 5] that the polynomial

$$q^{(\epsilon)}(x) = \frac{\sum_{i=1}^{l'} x^{2^{il}} + \epsilon}{x^{2^l+1}} \qquad \text{for} \quad \epsilon = 0, 1 \tag{3}$$

is a permutation polynomial on $\mathrm{GF}(2^k)^*$ if and only if $\epsilon \equiv l'+1 \pmod 2$. (To be formally more precise, we get a *polynomial* $q^{(\epsilon)}(x)$ if $x^{-(2^l+1)}$ is substituted by $x^{(2^k-1)-(2^l+1)}$.) In the sequel, we simply use $q(x)$ instead of $q^{(\epsilon)}(x)$ for $\epsilon \equiv l'+1 \pmod 2$. Moreover, $q(x)$ and $R(x^{-1})$ are inverses of each other [9, Theorem 6], i.e., for any nonzero $u, v \in \mathrm{GF}(2^k)$ with $q(u) = v^{-1}$ it always holds that $R(v) = u$. In (3) and in the rest of the paper, whenever a positive integer e is added to an element of $\mathrm{GF}(2^k)$, it means that added is the identity element of $\mathrm{GF}(2^k)$ times $e \pmod 2$.

In the general case when $\gcd(l,k) = d \geq 1$, let $k = nd$ for some $n > 1$ and introduce a particular sequence of polynomials over $\mathrm{GF}(2^k)$. For any $u \in \mathrm{GF}(2^k)$ denote $u_i = u^{2^{il}}$ for $i = 0, \ldots, n-1$ and let

$$\begin{aligned} C_1(x) &= 1\,, \\ C_2(x) &= 1\,, \\ C_{i+2}(x) &= C_{i+1}(x) + x_i C_i(x) \quad \text{for} \quad 1 \leq i \leq n-1\ . \end{aligned} \tag{4}$$

Lemma 1 *For any $u \in \mathrm{GF}(2^k)$ and $i \in \{1, \ldots, n-1\}$*

$$C_{i+2}(u) = C_{i+1}^{2^l}(u) + u_1 C_i^{2^{2l}}(u) \qquad \textit{and} \tag{5}$$

$$C_i^{2^l}(u) C_{i+2}(u) + C_{i+1}^{2^l+1}(u) = \prod_{j=1}^{i} u_j\ . \tag{6}$$

Proof. Both identities are proved using induction on i. For $i = 1$ and $i = 2$ the correctness is easily checked taking the definition. Assuming the

identities hold for $i < t$ we get for $i = t > 2$

$$\begin{aligned} C_{t+2}(u) &\overset{(4)}{=} C_{t+1}(u) + u_t C_t(u) \\ &= C_t^{2^l}(u) + u_1 C_{t-1}^{2^{2l}}(u) + u_t C_{t-1}^{2^l}(u) + u_t u_1 C_{t-2}^{2^{2l}}(u) \\ &= (C_t(u) + u_{t-1} C_{t-1}(u))^{2^l} + u_1 (C_{t-1}(u) + u_{t-2} C_{t-2}(u))^{2^{2l}} \\ &\overset{(4)}{=} C_{t+1}^{2^l}(u) + u_1 C_t(u)^{2^{2l}} \end{aligned}$$

and

$$\begin{aligned} & C_t^{2^l}(u) C_{t+2}(u) + C_{t+1}^{2^l+1}(u) \\ &\overset{(4)}{=} (C_{t-1}^{2^l}(u) + u_{t-1} C_{t-2}^{2^l}(u))(C_{t+1}(u) + u_t C_t(u)) + (C_t(u) + u_{t-1} C_{t-1}(u))^{2^l+1} \\ &= C_{t-1}^{2^l}(u) C_{t+1}(u) + C_t^{2^l+1}(u) + u_{t-1} u_t (C_{t-2}^{2^l}(u) C_t(u) + C_{t-1}^{2^l+1}(u)) \\ &\quad + u_{t-1} (C_{t-2}^{2^l}(u) C_{t+1}(u) + C_{t-1}(u) C_t^{2^l}(u)) \\ &= \prod_{j=1}^{t-1} u_j + \prod_{j=1}^{t} u_j \\ &\quad + u_{t-1} (C_{t-2}^{2^l}(u)(C_t(u) + u_{t-1} C_{t-1}(u)) + C_{t-1}(u)(C_{t-1}(u) + u_{t-2} C_{t-2}(u))^{2^l}) \\ &= \prod_{j=1}^{t-1} u_j + \prod_{j=1}^{t} u_j + u_{t-1}(C_{t-2}^{2^l}(u) C_t(u) + C_{t-1}^{2^l+1}(u)) = \prod_{j=1}^{t} u_j \ . \end{aligned}$$

(5) can be seen as an equivalent recursive definition of $C_i(x)$. □

We also define polynomials $Z_n(x)$ over $\mathrm{GF}(2^k)$ as $Z_1(x) = 1$ and

$$Z_n(x) = C_{n+1}(x) + x C_{n-1}^{2^l}(x) \tag{7}$$

for $n > 1$. Note that for any $u \in \mathrm{GF}(2^k)$ we get

$$\begin{aligned} Z_n^{2^l}(u) &\overset{(7)}{=} C_{n+1}^{2^l}(u) + u_1 C_{n-1}^{2^{2l}}(u) \\ &\overset{(4)}{=} C_n^{2^l}(u) + u_0 C_{n-1}^{2^l}(u) + u_1 C_{n-1}^{2^{2l}}(u) \\ &\overset{(5)}{=} C_{n+1}(u) + u_0 C_{n-1}^{2^l}(u) \\ &\overset{(7)}{=} Z_n(u) \end{aligned}$$

and thus, $Z_n(u) \in \mathrm{GF}(2^l)$. Since $\mathrm{GF}(2^k) \bigcap \mathrm{GF}(2^l) = \mathrm{GF}(2^d)$, we have $Z_n(u) \in \mathrm{GF}(2^d)$. The following lemma describes zeros of $C_n(x)$ in $\mathrm{GF}(2^k)$.

Proposition 1 *Take any $v \in \mathrm{GF}(2^{nd}) \setminus \mathrm{GF}(2^d)$ with $n > 1$ and let*

$$V = \frac{v_0^{2^{2l}+1}}{(v_0+v_1)^{2^l+1}} \ . \tag{8}$$

Then

$$C_n(V) = \frac{\mathrm{Tr}_d^{nd}(v_0)}{(v_1+v_2)} \prod_{j=2}^{n-1} \left(\frac{v_0}{v_0+v_1}\right)^{2^{jl}} \ .$$

If n is odd (resp. n is even) then the total number of distinct zeros of $C_n(x)$ in $\mathrm{GF}(2^{nd})$ is equal to $\frac{2^{(n-1)d}-1}{2^{2d}-1}$ (resp. $\frac{2^{(n-1)d}-2^d}{2^{2d}-1}$). All zeros have the form of (8) with $\mathrm{Tr}_d^{nd}(v_0) = 0$ and occur with multiplicity 2^l. Moreover, polynomial $C_n(x)$ splits in $\mathrm{GF}(2^{nd})$ if and only if $d = l$ or $n < 4$.

Proof. First, note that $\mathrm{GF}(2^{nd}) \bigcap \mathrm{GF}(2^l) = \mathrm{GF}(2^d)$ and $v \in \mathrm{GF}(2^{nd}) \setminus \mathrm{GF}(2^d)$ if and only if $v_0 \neq v_1$ which guarantees that the denominator in (8) and in the above identity for $C_n(V)$ is not zero. Now, using induction on i we prove that

$$C_i(V) = \frac{\sum_{j=1}^{i} v_j}{(v_1+v_2)} \prod_{j=2}^{i-1} \left(\frac{v_0}{v_0+v_1}\right)^{2^{jl}} \tag{9}$$

for $2 \leq i \leq n+1$. For $i = 2$ and $i = 3$ this identity is easily checked using the definition (4) of $C_i(x)$ (for $i = 2$, we assume the product over the empty set to be equal to 1). Assuming this identity holds for $i < t$ we get for $i = t > 3$

$$\begin{aligned}
C_t(V) &\overset{(4)}{=} C_{t-1}(V) + V_{t-2}C_{t-2}(V) \\
&= \frac{\sum_{j=1}^{t-1} v_j}{(v_1+v_2)} \prod_{j=2}^{t-2} \left(\frac{v_0}{v_0+v_1}\right)^{2^{jl}} + \frac{v_{t-2}^{2^{2l}+1} \sum_{j=1}^{t-2} v_j}{(v_{t-2}+v_{t-1})^{2^l+1}(v_1+v_2)} \prod_{j=2}^{t-3} \left(\frac{v_0}{v_0+v_1}\right)^{2^{jl}} \\
&= \frac{\left((v_{t-1}+v_t)\sum_{j=1}^{t-1} v_j + v_t \sum_{j=1}^{t-2} v_j\right) \prod_{j=2}^{t-2} v_0^{2^{jl}}}{(v_1+v_2)\prod_{j=2}^{t-1}(v_0+v_1)^{2^{jl}}} \\
&= \frac{\sum_{j=1}^{t} v_j}{(v_1+v_2)} \prod_{j=2}^{t-1} \left(\frac{v_0}{v_0+v_1}\right)^{2^{jl}} \ .
\end{aligned}$$

It remains to note that for $i = n$, in $\mathrm{GF}(2^{nd})$ we have $\sum_{j=1}^{n} v_j = \sum_{j=1}^{n} v^{2^{jd}} = \mathrm{Tr}_d^{nd}(v_0)$.

Obviously, $C_n(V) = 0$ if and only if $\mathrm{Tr}_d^{nd}(v_0) = 0$ which is equivalent to $v_0 = u + u^{2^l}$ for some $u \in \mathrm{GF}(2^{nd})$. This easily follows from the fact that the linear operator $L(u) = u + u^{2^l}$ on $\mathrm{GF}(2^{nd})$ has the kernel of dimension d and, thus, the number of elements in the image of L is $2^{d(n-1)}$. For any $u \in \mathrm{GF}(2^{nd})$ we have $\mathrm{Tr}_d^{nd}(u + u^{2^l}) = 0$ leading to the conclusion that the image of L contains all the elements of $\mathrm{GF}(2^{nd})$ having zero trace in $\mathrm{GF}(2^d)$ since the total number of such elements is exactly $2^{d(n-1)}$. Moreover, $u \notin \mathrm{GF}(2^{2d})$ since $v_0 \in \mathrm{GF}(2^d) \subseteq \mathrm{GF}(2^l)$ if and only if the corresponding $u \in \mathrm{GF}(2^{2l})$ and since $\mathrm{GF}(2^{nd}) \cap \mathrm{GF}(2^{2l}) = \mathrm{GF}(2^{d\gcd(n,2)})$. It follows from the proof of Proposition 5 that the mapping from $u \in \mathrm{GF}(2^{nd}) \setminus \mathrm{GF}(2^{2d})$ via $v_0 = u + u^{2^l}$ to $V \in \mathrm{GF}(2^{nd})^*$ defined by (8) is $(2^{3d} - 2^d)$-to-1. Therefore, we have found $\frac{|\mathrm{GF}(2^{nd}) \setminus \mathrm{GF}(2^{2d})|}{2^{3d}-2^d}$ distinct zeros of $C_n(x)$ in $\mathrm{GF}(2^{nd})$ and if n is odd (resp. n is even) then this number is equal to $\frac{2^{(n-1)d}-1}{2^{2d}-1}$ (resp. $\frac{2^{(n-1)d}-2^d}{2^{2d}-1}$).

It is easy to check by induction that if i is odd (resp. i is even) then the algebraic degree of polynomials $C_i(x)$ is equal to $\frac{2^{il}-2^l}{2^{2l}-1}$ (resp. $\frac{2^{il}-2^{2l}}{2^{2l}-1}$) since

$$\deg C_{i+2}(x) = \max\{\deg C_{i+1}(x), 2^{il} + \deg C_i(x)\} = 2^{il} + \deg C_i(x) \ .$$

Further, if we define the sequence of polynomials $C'_i(x)$ for $i = 1, \ldots, n$ with $C'_1(x) = C'_2(x) = 1$ and $C'_{i+2}(x) = C'_{i+1}(x) + x_{i-1}C'_i(x)$ then $C_i(x) = C'_i(x)^{2^l}$ for $i = 1, \ldots, n$. Therefore, all zeros of $C_n(x)$ have multiplicity at least 2^l. Now it is clear that the number of zeros having the form of (8) with $\mathrm{Tr}_d^{nd}(v_0) = 0$ multiplied by 2^l is equal to the degree of $C_n(x)$ if and only if $d = l$ or $n < 4$.

It means that $C_n(x)$ splits in $\mathrm{GF}(2^{nl})$ and zeros of $C_n(x)$ in $\mathrm{GF}(2^{nd})$ are exactly the elements obtained by (8) using $w_0 \in \mathrm{GF}(2^{nl}) \setminus \mathrm{GF}(2^l)$ with $\mathrm{Tr}_l^{nl}(w_0) = 0$ that result in $V \in \mathrm{GF}(2^{nd})$. It also follows from the proof of Proposition 5 that polynomial $f_b(y) = y^{2^l+1} + by + b$ with $b \in \mathrm{GF}(2^{nd})^*$ has exactly $2^d + 1$ zeros in $\mathrm{GF}(2^{nd})$ if and only if b^{-1} has the form of (8) with $\mathrm{Tr}_d^{nd}(v_0) = 0$. Take any $V \in \mathrm{GF}(2^{nd})$ obtained by (8) using $w_0 \in \mathrm{GF}(2^{nl}) \setminus \mathrm{GF}(2^l)$ with $\mathrm{Tr}_l^{nl}(w_0) = 0$. Then $f_{V^{-1}}(y)$ splits in $\mathrm{GF}(2^{nl})$ and, by [5, Corollary 7.2], this is equivalent to $f_{V^{-1}}(y)$ having 2^d+1 zeros in $\mathrm{GF}(2^{nd})$. Thus, there exists some $v_0 \in \mathrm{GF}(2^{nd}) \setminus \mathrm{GF}(2^d)$ with $\mathrm{Tr}_d^{nd}(v_0) = 0$ that gives this V using (8). □

Corollary 1 *If n is odd (resp. n is even) then the total number of distinct zeros of $Z_n(x)$ in $\mathrm{GF}(2^{nd})$ is equal to $\frac{2^{(n+1)d}-2^{2d}}{2^{2d}-1}$ (resp. $\frac{2^{(n+1)d}-2^d}{2^{2d}-1}$). All zeros have the form of (8) and occur with multiplicity one. Moreover, polynomial $Z_n(x)$ splits in $\mathrm{GF}(2^{nd})$ if and only if $d = l$ or $n = 1$.*

PROOF. Using (9), it can be verified directly that $C_{n+1}(V) = VC_{n-1}^{2^l}(V)$ for any $V \in \mathrm{GF}(2^{nd})$ having the form of (8) (the case $n = 2$ is easily checked having the definition of $C_i(x)$). Also, knowing the algebraic degree of polynomials $C_i(x)$ from the proof of Proposition 1, we conclude that

$$\deg(Z_n(x)) = \deg C_{n+1}(x)$$

and is equal to $\frac{2^{(n+1)l}-2^{2l}}{2^{2l}-1}$ (resp. $\frac{2^{(n+1)l}-2^{l}}{2^{2l}-1}$) if n is odd (resp. n is even). Denote

$$S = \{x \in \mathrm{GF}(2^{nd}) \setminus \mathrm{GF}(2^d) \mid \mathrm{Tr}_d^{nd}(x) \neq 0\} \ . \tag{10}$$

It follows from the proof of Proposition 4 that the mapping from $v \in S$ to $V \in \mathrm{GF}(2^{nd})^*$ defined by (8) is (2^d-1)-to-1. Recalling the corresponding fact from the latest proof, we conclude that the total number of distinct values of V obtained by (8) is equal to $\frac{|\mathrm{GF}(2^{nd})\setminus\mathrm{GF}(2^{2d})|}{2^{3d}-2^d} + \frac{|S|}{2^d-1}$ being identical to the degree of $Z_n(x)$ if and only if $d = l$ or $n = 1$. Note that two different values of $v \in \mathrm{GF}(2^{nd}) \setminus \mathrm{GF}(2^d)$ with zero and nonzero trace in $\mathrm{GF}(2^d)$ can not map to the same value V using (8) since $C_n(V) = 0$ if and only if the trace of the corresponding v is also equal zero.

It means that that $Z_n(x)$ splits in $\mathrm{GF}(2^{nl})$ and its zeros in $\mathrm{GF}(2^{nd})$ are exactly the elements obtained by (8) using $w_0 \in \mathrm{GF}(2^{nl}) \setminus \mathrm{GF}(2^l)$ that result in $V \in \mathrm{GF}(2^{nd})$. It also follows from the proof of Propositions 4 and 5 that polynomial $f_b(y) = y^{2^l+1} + by + b$ with $b \in \mathrm{GF}(2^{nd})^*$ has exactly one or 2^d+1 zeros in $\mathrm{GF}(2^{nd})$ if and only if b^{-1} has the form of (8). Take any $V \in \mathrm{GF}(2^{nd})$ obtained by (8) using $w_0 \in \mathrm{GF}(2^{nl}) \setminus \mathrm{GF}(2^l)$. Then $f_{V^{-1}}(y)$ has exactly one or $2^l + 1$ zeros $\mathrm{GF}(2^{nl})$ and, by [5, Corollaries 7.2, 7.3], this is equivalent to $f_{V^{-1}}(y)$ having one or 2^d+1 zeros in $\mathrm{GF}(2^{nd})$ respectively. Thus, there exists some $v_0 \in \mathrm{GF}(2^{nd}) \setminus \mathrm{GF}(2^d)$ that gives this V using (8). □

Corollary 2 *For any $V \in \mathrm{GF}(2^k)$ having the form of (8) with $n > 2$ and $\mathrm{Tr}_d^k(v_0) \neq 0$ we have $\mathrm{Tr}_d^k\left(C_{n-1}^{2^l}(V)/C_n^{2^l+1}(V)\right) = 0$.*

PROOF. Using (9), it can be verified directly that

$$\frac{C_{n-1}^{2^l}(V)}{C_n^{2^l+1}(V)} = \mathrm{N}_d^k\left(1 + \frac{v_1}{v_0}\right)\frac{v_1\sum_{j=2}^n v_j}{\mathrm{Tr}_d^k(v_0)^2}$$

for any $V \in \mathrm{GF}(2^k)$ having the form of (8) and $n > 2$. Now note that

$$\mathrm{Tr}_d^k\Big(v_1\sum_{j=2}^n v_j\Big) = \mathrm{Tr}_d^k\left(v_1\mathrm{Tr}_d^k(v_0) + v_1^2\right) = \mathrm{Tr}_d^k(v_0)^2 + \mathrm{Tr}_d^k(v_0^2) = 0$$

and we are done. $\square$

Value of $C_i(x)$ is equal to the determinant of a three-diagonal symmetric matrix (note a comprehensive study of such matrices in [10]). Indeed, for any $u \in \mathrm{GF}(2^k)$ and $j \le i$ let $\Delta_u(j,i)$ denote the determinant of matrix D of size $i-j+2$ that contains ones on the main diagonal and with $D(t,t+1) = D(t+1,t) = u_{j+t-1}$ for $t = 1,\ldots,i-j+1$, where the indices of u_i are reduced modulo n. Expanding the determinant of D by minors along the last row we obtain

$$\Delta_u(j,i) = \Delta_u(j,i-1) + u_i^2 \Delta_u(j,i-2) \tag{11}$$

assuming $\Delta_u(j,i) = 1$ if $i-j \in \{-2,-1\}$. Comparing the latter recursive identity with (4) it is easy to see that

$$\Delta_u(1,i) = C_{i+2}^2(u) \ . \tag{12}$$

Moreover, from the definition of the determinant it also follows that

$$\Delta_u(1,i)^{2^{tl}} = \Delta_u(1+t,i+t) \quad \text{for} \quad 0 \le t \le n-1 \ . \tag{13}$$

Now assume $d = \gcd(l,k) = 1$ and consider V having the form of (8) as a function of $x \in \mathrm{GF}(2^k)^{**}$ denoted $V(x)$. It is interesting that $V(x)$ is closely related to polynomial mappings $q^{(\epsilon)}(x)$ defined in (3). In particular, this connection leads to new properties of $q^{(\epsilon)}(x)$, with $\epsilon \equiv l' \pmod 2$, when it is not a permutation. Denote

$$\mathcal{T}_i = \{x \in \mathrm{GF}(2^k)^{**} \mid \mathrm{Tr}_k(x) = i\} \quad \text{for} \quad i = 0,1$$

and let $V(\mathcal{T}_i)$ and $q^{(\epsilon)}(\mathcal{T}_i)$ denote multisets containing all elements (with repetitions) in the image of $\mathcal{T}_i$ under the corresponding mapping $V(x)$ or $q^{(\epsilon)}(x)$.

Corollary 3 *Take $\epsilon \equiv l' \pmod 2$. Then $q^{(\epsilon)}(\mathcal{T}_i) = V(\mathcal{T}_0)$, where $i \equiv k \pmod 2$, and $q^{(\epsilon)}(x)$ defines a 3-to-1 mapping on $\mathcal{T}_i$. Also, if k is odd then $q^{(0)}(\mathcal{T}_0) = V(\mathcal{T}_1)$ and $q^{(0)}(x)$ defines an injective mapping on $\mathcal{T}_0$.*

Proof. It follows from the proof of Proposition 1 and Corollary 1 that $V(x)$ defines a 3-to-1 mapping on $\mathcal{T}_0$ and is injective on $\mathcal{T}_1$. This *does not* mean that $V(\mathcal{T}_i) \subset \mathcal{T}_i$ for $i = 0,1$ in the sense of a normal subset relation.

Taking any $x_0 \in \mathrm{GF}(2^k)^{**}$ denote $\Delta = (x_0^{2^l-1} + x_0^{-1})^{-1/(2^l-1)}$ and $\lambda = x_0\Delta$. It is easy to check that $\lambda + \lambda^{2^l} = \Delta^{2^l}$. Thus, $\mathrm{Tr}_k(\Delta) = 0$ and Δ defines a

2-to-1 mapping of $\mathrm{GF}(2^k)^{**}$ on $\mathcal{T}_0$ if k is odd and on $\mathcal{T}_0 \bigcup \{1\}$ if k is even. Therefore,

$$V(\mathcal{T}_0) = \left\{ V\big((x_0^{2^l-1} + x_0^{-1})^{-\frac{1}{2^l-1}}\big) \mid x_0 \in \mathrm{GF}(2^k)^{**},\ x_0^{2^l} + x_0 \neq 1 \right\} \quad \text{and}$$

$$V\big((x_0^{2^l-1} + x_0^{-1})^{-\frac{1}{2^l-1}}\big) = \frac{x_0^{2^l}(x_0^{2^l}+1)}{(x_0^{2^l}+x_0+1)^{2^l+1}} = \frac{\sum_{i=1}^{l'} z_0^{2^{il}} + l'}{z_0^{2^l+1}} = q^{(\epsilon)}(z_0) \ ,$$

where $z_0 = x_0^{2^l} + x_0 + 1 \in \mathcal{T}_i$ with $\epsilon \equiv l' \pmod 2$ and $i \equiv k \pmod 2$. Note that l' and k can not be both even and $\epsilon = i = 0$ is impossible. Here we used that $V(x) = x^{1-2^l}/(x^{1-2^l}+1)^{2^l+1}$ which is easily obtained from (8). Finally,

$$q^{(\epsilon)}(\mathcal{T}_i) = \left\{ q^{(\epsilon)}\big(x_0^{2^l} + x_0 + 1\big) \mid x_0 \in \mathrm{GF}(2^k)^{**},\ x_0^{2^l} + x_0 \neq 1 \right\}$$

and $x^{2^l} + x + 1$ defines a 2-to-1 mapping of $\mathrm{GF}(2^k)^{**}$ on $\mathcal{T}_1$ if k is odd and on $\mathcal{T}_0 \bigcup \{0\}$ if k is even.

Define $T_l(x) = \sum_{i=0}^{l-1} x^{2^i}$ on $\mathrm{GF}(2^k)$ that is a permutation polynomial if l is odd and 2-to-1 mapping if l is even. This follows from the fact that $T_l(x)$ is linearized and $T_l(x) = 0$ has the only solution $x = 0$ if l is odd and two solutions $x = 0, 1$ if l is even (note that $(T_l(x)+1)T_l(x) = x + x^{2^l}$). Therefore, $T_l(x)$ is a permutation of $\mathcal{T}_0$ for any l and odd k since $\mathrm{Tr}_k(T_l(x)) = 0$ if l is even (in this case $T_l(x) = T_l(x+1)$) and is equal to $\mathrm{Tr}_k(x)$ if l is odd.

Dickson polynomial number 2^l+1 can be written as $D_{2^l+1}(x) = x^{2^l+1}(1 + T_l(x^{-1})^2)$ (see, for instance, [7]). If k is odd then $\gcd(2^l+1, 2^k-1) = 1$ and, by [7], $D_{2^l+1}(x)$ is a permutation on $\mathcal{H}_0$. Thus, $D_{2^l+1}(x^{-1})^{-1}$ is a permutation on $\mathcal{T}_0$. Note that

$$D_{2^l+1}(x^{-1})^{-1} = \frac{x^{2^l+1}}{T_l(x)^2+1} = \frac{x}{T_l(x)+1} + \left(\frac{x}{T_l(x)+1}\right)^2 + x \ .$$

Therefore, if k is odd then

$$V(\mathcal{T}_1) = \left\{ \frac{(T_l(x)+1)^{2^{2k}+1}}{\big(T_l(x) + T_l^{2^k}(x)\big)^{2^k+1}} \mid x_0 \in \mathcal{T}_0 \right\} \quad \text{and}$$

$$q^{(0)}(T_l(x_0)) =$$

3. Zeros of $P_a(x)$ when $\gcd(l, k) = 1$

In this section, we analyze the zeros in $\mathrm{GF}(2^k)$ of the polynomial $P_a(x)$ assuming that l and k are coprime integers with $l < k$. In this case, denote

$l' = l^{-1} \pmod{k}$ and take $R(x)$ defined in (2). The following Lemma 2 easily follows from the earlier mentioned fundamental result on permutation polynomials due to Dobbertin.

Also note the fact that since $l'l \equiv 1 \pmod{k}$ then

$$(2^l - 1)(1 + 2^l + 2^{2l} + \cdots + 2^{(l'-1)l}) = 2^{ll'} - 1 \equiv 1 \pmod{2^k - 1} \ .$$

Therefore, $u^{2^{l'l}} = u^2$ for any $u \in \mathrm{GF}(2^k)$ and this identity will be used repeatedly further in the proofs.

Lemma 2 *Take $F_a(x)$ defined in (1). Then for any $a \in \mathrm{GF}(2^k)^*$, the element $\mathcal{V} = R(a^{-1})$ is a zero of $F_a(x)$ in $\mathrm{GF}(2^k)$.*

Proof. Since $q(x)$ from (3) is a permutation polynomial on $\mathrm{GF}(2^k)^*$, then for any fixed $a \in \mathrm{GF}(2^k)^*$ the equation

$$ax^{2^l+1} = \sum_{i=1}^{l'} x^{2^{il}} + l' + 1 \tag{14}$$

has exactly one solution $\mathcal{V} = R(a^{-1})$ in $\mathrm{GF}(2^k)^*$. Raising (14) to the power of 2^l results in

$$a^{2^l} x^{2^{2l}+2^l} = \sum_{i=2}^{l'+1} x^{2^{il}} + l' + 1 = \sum_{i=2}^{l'} x^{2^{il}} + x^{2^{l+1}} + l' + 1 \ .$$

The latter identity, after being added to (14) and setting $x = \mathcal{V}$, gives

$$a\mathcal{V}^{2^l+1} = a^{2^l}\mathcal{V}^{2^{2l}+2^l} + \mathcal{V}^{2^l} + \mathcal{V}^{2^{l+1}}$$

and consecutively, since $\mathcal{V} \neq 0$, $F_a(\mathcal{V}) = a^{2^l}\mathcal{V}^{2^{2l}} + \mathcal{V}^{2^l} + a\mathcal{V} + 1 = 0$. □

Now we introduce a particular sequence of polynomials over $\mathrm{GF}(2^k)$ and prove some important properties of these that will be used further for getting the main result of this section about zeros of $P_a(x)$. Denote

$$e(i) = 1 + 2^l + 2^{2l} + \cdots + 2^{(i-1)l}, \quad \text{for} \quad i = 1, \ldots, l'$$

so, in particular, $e(l') = (2^l - 1)^{-1} \pmod{2^k - 1}$. Now take every additive term x^e with $e \neq 0$ in the polynomial $1 + (1 + x)^{e(i)}$ and replace the exponent

e with the cyclotomic equivalent number obtained by shifting the binary expansion of e maximally (till you get an odd number) in the direction of the least significant bits. We call this *reduction* procedure. Recall that two exponents e_1 and e_2 are cyclotomic equivalent if $2^i e_1 \equiv e_2 \pmod{2^k - 1}$ for some $i < k$. For instance, $x^{2^{il}}$ is reduced to x and $x^{2^{il}+2^{jl}}$ is reduced to $x^{1+2^{(j-i)l}}$ if $i < j$ and so on. The obtained reduced polynomials are denoted as $H_i(x)$ and we use square brackets to denote application of the described reduction procedure to a polynomial, so $H_i(x) = [1 + (1 + x)^{e(i)}]$ for $i = 1, \ldots, l'$. The first few polynomials in the sequence (after eliminating all pairs of equal terms) are

$$\begin{aligned}
H_1(x) &= x \\
H_2(x) &= [x + x^{2^l} + x^{1+2^l}] = x + x + x^{1+2^l} = x^{1+2^l} \\
H_3(x) &= [x + x^{2^l} + x^{2^{2l}} + x^{1+2^l} + x^{1+2^{2l}} + x^{2^l+2^{2l}} + x^{1+2^l+2^{2l}}] \\
&= x + x + x + x^{1+2^l} + x^{1+2^{2l}} + x^{1+2^l} + x^{1+2^l+2^{2l}} \\
&= x + x^{1+2^{2l}} + x^{1+2^l+2^{2l}} \ .
\end{aligned}$$

Lemma 3 *If polynomials $H_i(x)$ are defined as above then*

$$\mathrm{Tr}_k(H_i(x)) = \mathrm{Tr}_k\big(1 + (1 + x)^{e(i)}\big)$$

for any $x \in \mathrm{GF}(2^k)$ and $i = 1, \ldots, l'$. Also let

$$Q(x) = (x_0^{2^l+1} + x_0)x^{2^l} + x_0^2 x + x_0$$

for any $x_0 \in \mathrm{GF}(2^k)^*$. Then

$$Q(H_{l'}(x_0^{-1})) = (1 + x_0)(1 + x_0^{-1})^{e(l')} \ .$$

Proof. Obviously, we get the trace identity for $H_{l'}(x)$ from the definition. Further,

$$\begin{aligned}
H_i(x) &= [1 + (1 + x)^{e(i)}] \\
&= [1 + (1 + x)^{e(i-1)}(1 + x)^{2^{(i-1)l}}] \\
&= [H_{i-1}(x) + x^{2^{(i-1)l}}(1 + x)^{e(i-1)}] \\
&\overset{(*)}{=} x(1 + x)^{e(i)-1} + H_{i-1}(x) \ ,
\end{aligned}$$

where $(*)$ follows from the following argumentation. First, note that the exponents of additive terms in $x(1 + x)^{e(i)-1}$ are exactly all 2^{i-1} distinct

integers of the form $1+t_1 2^l+\cdots+t_{i-1}2^{(i-1)l}$ with $t_j \in \{0,1\}$ for $j=1,\ldots,i-1$ and the reduction does not apply to any of these so

$$[x(1+x)^{e(i)-1}] = x(1+x)^{e(i)-1} \ .$$

On the other hand, the number of terms in $[x^{2^{(i-1)l}}(1+x)^{e(i-1)}]$ is also equal to 2^{i-1} since the exponents in these terms are exactly all the integers of the form $t_0 + t_1 2^l + \cdots + t_{i-2}2^{(i-2)l} + 2^{(i-1)l}$ with $t_j \in \{0,1\}$ for $j=0,\ldots,i-2$ and none of these become equal after the reduction. Moreover, every such an exponent, after reduction, can be found in $x(1+x)^{e(i)-1}$ so

$$[x^{2^{(i-1)l}}(1+x)^{e(i-1)}] = x(1+x)^{e(i)-1} \ .$$

Also note that all terms of $H_{i-1}(x)$ are also present in $x(1+x)^{e(i)-1}$. Thus, the number of terms in $H_i(x)$ that remain after eliminating all pairs of equal terms and denoted as $\#H_i$ is equal to $2^{i-1} - \#H_{i-1}$. Unfolding the obtained recursive expression for $H_i(x)$ starting from $H_1(x) = x$ we get that

$$H_i(x) = x(1 + (1+x)^{2^l} + (1+x)^{2^l+2^{2l}} + \cdots + (1+x)^{e(i)-1}) \ . \tag{15}$$

Now we can evaluate

$$\begin{aligned}
&Q(H_{l'}(x_0^{-1})) \\
&= (x_0^{2^l+1} + x_0) H_{l'}(x_0^{-1})^{2^l} + x_0^2 H_{l'}(x_0^{-1}) + x_0 \\
&= (x_0 + x_0^{-2^l+1}) \left(1 + (1+x_0^{-1})^{2^{2l}} + (1+x_0^{-1})^{2^{2l}+2^{3l}} + \cdots + (1+x_0^{-1})^{2^{2l}+\cdots+2^{l'l}}\right) \\
&\quad + x_0 \left(1 + (1+x_0^{-1})^{2^l} + (1+x_0^{-1})^{2^l+2^{2l}} + \cdots + (1+x_0^{-1})^{e(l')-1}\right) + x_0 \\
&= \left((x_0 + x_0^{-2^l+1}) + x_0(1+x_0^{-1})^{2^l}\right) \left(1 + (1+x_0^{-1})^{2^{2l}} + \cdots + (1+x_0^{-1})^{2^{2l}+\cdots+2^{(l'-1)l}}\right) \\
&\quad + (x_0 + x_0^{-2^l+1})(1+x_0^{-1})^{2^{2l}+\cdots+2^{l'l}} + x_0 + x_0 \\
&= x_0(1+x_0^{-1})^{2^l+2^{2l}+\cdots+2^{l'l}} \\
&= x_0(1+x_0^{-1})^{2+2^l+2^{2l}+\cdots+2^{(l'-1)l}} \\
&= (1+x_0)(1+x_0^{-1})^{e(l')}
\end{aligned}$$

as claimed. □

Lemma 4 *For any $a \in \mathrm{GF}(2^k)^*$ let $x_0 \in \mathrm{GF}(2^k)$ satisfy $x_0^{2^l+1} + x_0 = a$. Then*

$$\mathrm{Tr}_k\big(1 + (1+x_0^{-1})^{e(l')}\big) = \mathrm{Tr}_k(R(a^{-1})) \ .$$

PROOF. Denote $\Gamma = x_0^{2^l-1} + x_0^{-1}$ (obviously $\Gamma \neq 0$ since $x_0 \neq 1$), $\Delta = \Gamma^{-e(l')}$, and further, using Lemma 3, evaluate

$$Q(H_{l'}(x_0^{-1}))x_0^{e(l')} = (1+x_0)(1+x_0)^{e(l')} = (1+x_0^{2^l})^{e(l')}$$

and thus, $Q(H_{l'}(x_0^{-1}))^{2^l-1} = \Gamma$ or, equivalently,

$$Q(H_{l'}(x_0^{-1})) = \Delta^{-1} \ . \tag{16}$$

In what follows, we use the technique suggested by Dobbertin for proving [9, Theorem 1]. Take the polynomial $F_a(x)$ defined in (1) and note that

$$\begin{aligned} F_a(x) &= a^{2^l} x^{2^{2l}} + x^{2^l} + ax + 1 \\ &= a^{2^l} x^{2^{2l}} + x_0^{2^{l+1}} x^{2^l} + x_0^{2^l} + (x_0^{2^l-1} + x_0^{-1}) \left((x_0^{2^l+1} + x_0) x^{2^l} + x_0^2 x + x_0 \right) \\ &= Q(x)^{2^l} + \Gamma Q(x) = Q(x) \left(Q(x)^{2^l-1} + \Delta^{-(2^l-1)} \right) \end{aligned}$$

for $x_0^{2^l+1} + x_0 = a$ and, therefore, by (16), $F_a(H_{l'}(x_0^{-1})) = 0$. Consider the equation

$$Q(x) + \Delta^{-1} = 0 \tag{17}$$

whose roots are also the zeros of $F_a(x)$. We will show that (17) has exactly two roots with $H_{l'}(x_0^{-1})$ and $R(a^{-1})$ being among them (however, we do not claim that $R(a^{-1}) \neq H_{l'}(x_0^{-1})$). Multiplying (17) by $\mu = (x_0^2\Delta)^{-1}$ and using that $(x_0^{2^l+1} + x_0)\Delta^{2^l-1} = x_0^2$ gives

$$\mu((x_0^{2^l+1} + x_0)x^{2^l} + x_0^2 x + x_0 + \Delta^{-1}) = (x/\Delta)^{2^l} + x/\Delta + x_0\mu + x_0^2\mu^2 = 0 \ ,$$

which has exactly two solutions $z_0 = H_{l'}(x_0^{-1})$ (see (16)) and $z_1 = H_{l'}(x_0^{-1}) + \Delta$, since its linearized homogeneous part $(x/\Delta)^{2^l} + x/\Delta$ has exactly two roots $x = 0$ and $x = \Delta$. Thus

$$z_0 + z_1 = \Delta = \left(\frac{x_0}{1 + x_0^{2^l}} \right)^{e(l')} \ .$$

Using $(x_0^{2^l} + 1)\Delta^{2^l-1} = x_0$ it is easy to see that $\Delta^{2^l} = x_0\Delta + (x_0\Delta)^{2^l}$ and we have $\mathrm{Tr}_k(\Delta) = 0$.

Now we show that none of the possible roots of $Q(x) = 0$ is a solution of (14). In fact, suppose that $Q(z) = 0$. Then, since $x_0 \neq 0$, we have

$z^{2^l} = (x_0 z)^{2^l} + x_0 z + 1$ and $az^{2^l} = x_0^2 z + x_0$ (since $a = x_0^{2^l+1} + x_0$). We put such a z into (14) and compute

$$\begin{aligned} & az^{2^l+1} + \sum_{i=1}^{l'} z^{2^{il}} + l' + 1 \\ & = (x_0^2 z + x_0) z + \sum_{i=0}^{l'-1} (x_0 z)^{2^{il}} + \sum_{i=1}^{l'} (x_0 z)^{2^{il}} + l' + l' + 1 \\ & = 1 \ . \end{aligned}$$

Therefore, recalling the proved identity $F_a(x) = Q(x)(Q(x)^{2^l-1} + \Delta^{-(2^l-1)})$ and keeping in mind that $\gcd(2^l - 1, 2^k - 1) = 1$ we see that $\mathcal{V} = R(a^{-1})$ which is the unique solution of (14) and, by Lemma 2, also the root of $F_a(x) = 0$, satisfies $Q(\mathcal{V}) = \Delta^{-1}$. Recall that (17) has exactly two solutions $z_0 = H_{l'}(x_0^{-1})$ and $z_1 = H_{l'}(x_0^{-1}) + \Delta$. Thus, $R(a^{-1}) + H_{l'}(x_0^{-1}) = \Delta$ or $R(a^{-1}) = H_{l'}(x_0^{-1})$ (although we do not need in our proof that $R(a^{-1}) \neq H_{l'}(x_0^{-1})$, we believe that this holds) and, by Lemma 3

$$\mathrm{Tr}_k(R(a^{-1})) = \mathrm{Tr}_k(H_{l'}(x_0^{-1})) = \mathrm{Tr}_k(1 + (1 + x_0^{-1})^{e(l')})$$

as claimed. □

Theorem 1 *For any $a \in \mathrm{GF}(2^k)^*$ and a positive integer $l < k$ with $\gcd(l, k) = 1$ polynomial $P_a(x)$ has either none, one, or three zeros in $\mathrm{GF}(2^k)$. Further, $P_a(x)$ has exactly one zero in $\mathrm{GF}(2^k)$ if and only if $\mathrm{Tr}_k(R(a^{-1}) + 1) = 1$, where $R(x)$ is defined in (2). Moreover, if $P_a(x_0) = 0$ for some $x_0 \in \mathrm{GF}(2^k)$ then*

$$\mathrm{Tr}_k(R(a^{-1})) = \mathrm{Tr}_k(H_{l'}(x_0^{-1})) = \mathrm{Tr}_k((1 + x_0^{-1})^{e(l')} + 1)$$

where polynomials $H_i(x)$ are defined in (15). Finally, the following distribution holds for k odd (resp. k even)

$$\begin{array}{lcll} M_0 & = & \frac{2^k+1}{3} & (\textit{resp. } \frac{2^k-1}{3}) \\ M_1 & = & 2^{k-1} - 1 & (\textit{resp. } 2^{k-1}) \\ M_3 & = & \frac{2^{k-1}-1}{3} & (\textit{resp. } \frac{2^{k-1}-2}{3}) \ . \end{array}$$

Proof. Assume $P_a(x_0) = 0$ for some $x_0 \in \mathrm{GF}(2^k)$. Now we substitute x in $P_a(x)$ with $x + x_0$ to get

$$(x + x_0)^{2^l+1} + (x + x_0) + a = 0$$

or

$$x^{2^l+1} + x_0 x^{2^l} + x_0^{2^l} x + x_0^{2^l+1} + x + x_0 + a = 0$$

which implies

$$x^{2^l+1} + x_0 x^{2^l} + (x_0^{2^l} + 1)x = 0 \ .$$

Since $x = 0$ corresponds to x_0 being the zero of $P_a(x)$, we can divide the latter equation by x. Further, after substituting $y = x^{-1}$ we note that $P_a(x)$ has i zeros if and only if the reciprocal equation, given by

$$(x_0^{2^l} + 1)y^{2^l} + x_0 y + 1 = 0 \tag{18}$$

has $i - 1$ zeros. This affine equation has either zero roots in $\mathrm{GF}(2^k)$ or the same number of roots as its homogeneous part $(x_0^{2^l} + 1)y^{2^l} + x_0 y$ which is seen to have exactly two solutions, the zero solution and a unique nonzero solution, since $\gcd(2^l - 1, 2^k - 1) = 1$. Therefore, it can be concluded that $P_a(x) = 0$ can have either zero, one, or three solutions in $\mathrm{GF}(2^k)$.

Now we need to find the conditions when there exists a solution of (18). Let $y = tw$, where $t^{2^l-1} = c$ and $c = \frac{x_0}{x_0^{2^l}+1}$. Since $\gcd(2^l - 1, 2^k - 1) = 1$, there is a one-to-one correspondence between t and c. Then (18) is equivalent to

$$w^{2^l} + w + \frac{1}{ct(x_0^{2^l} + 1)} = 0 \ .$$

Hence, (18) has no solutions if and only if

$$\mathrm{Tr}_k\left(\frac{1}{ct(x_0^{2^l} + 1)}\right) = 1 \ .$$

This easily follows from the fact that the linear operator $L(\omega) = \omega^{2^l} + \omega$ on $\mathrm{GF}(2^k)$ has the kernel of dimension one and, thus, the number of elements in the image of L is 2^{k-1}. For any $\omega \in \mathrm{GF}(2^k)$, we have $\mathrm{Tr}_k(\omega^{2^l} + \omega) = 0$ leading to the conclusion that the image of L contains all the elements in $\mathrm{GF}(2^k)$ having trace zero since the total number of such elements in $\mathrm{GF}(2^k)$ is exactly 2^{k-1}.

Since $c = t^{2^l-1}$ then $t = c^{1+2^l+2^{2l}+\cdots+2^{(l'-1)l}}$. Thus, from the definition of c

and t we get

$$\begin{aligned}
\mathrm{Tr}_k\left(\frac{1}{ct(x_0^{2^l}+1)}\right) &= \mathrm{Tr}_k\left(\left(\frac{x_0^{2^l}+1}{x_0}\right)^{1+e(l')}\left(\frac{1}{x_0^{2^l}+1}\right)\right) \\
&= \mathrm{Tr}_k\left(\frac{(x_0^{2^l}+1)^{e(l')}}{x_0^{1+e(l')}}\right) \\
&= \mathrm{Tr}_k\left(\frac{(x_0+1)^{2^l e(l')}}{x_0^{2^l e(l')}}\right) \\
&= \mathrm{Tr}_k\big((1+x_0^{-1})^{e(l')}\big) \ .
\end{aligned}$$

We conclude that $P_a(x)$ has exactly one zero in $\mathrm{GF}(2^k)$ (which is x_0) if and only if

$$\mathrm{Tr}_k\big((1+x_0^{-1})^{e(l')}\big) = 1 \tag{19}$$

or, equivalently, for all such a that $a = x_0^{2^l+1} + x_0$ with (19) holding. Combining this with the result of Lemma 4, we conclude that $P_a(x)$ has exactly one zero in $\mathrm{GF}(2^k)$ if and only if

$$\mathrm{Tr}_k(R(a^{-1})+1) = 1$$

(the "if" part follows from the fact that $R(x)$ is a permutation polynomial and seeing the value of M_1 that is computed in the next paragraph). In the case of none or three zeros, $\mathrm{Tr}_k(R(a^{-1})+1) = 0$. The trace identities follow from Lemmas 3 and 4.

Now note that since $e(l') = 1 + 2^l + 2^{2l} + \cdots + 2^{(l'-1)l}$ is invertible modulo $2^k - 1$ with the multiplicative inverse equal to $2^l - 1$ then $\gcd(e(l'), 2^k - 1) = 1$ and thus, $x \mapsto (1+x^{-1})^{e(l')}$ is a one-to-one mapping of $\mathrm{GF}(2^k)^*$ onto $\mathrm{GF}(2^k) \setminus \{1\}$. Therefore, if k is odd (resp. k is even) then the number of $x_0 \in \mathrm{GF}(2^k)^*$ satisfying (19) is equal to $2^{k-1} - 1$ (resp. 2^{k-1}) and obviously $x_0 \neq 1$. This also gives the value of M_1 since every x_0 satisfying (19) provides a unique $a = x_0^{2^l+1} + x_0 \in \mathrm{GF}(2^k)^*$ such that $P_a(x)$ has exactly one zero. Now note that if $a = 0$ then $P_a(x) = x^{2^l+1} + x + a$ has exactly two zeros $x = \{0, 1\}$. Thus, considering the mapping $x \mapsto x^{2^l+1} + x$ for x running through $\mathrm{GF}(2^k) \setminus \{0, 1\}$ it is easy to see that $M_1 + 3M_3 = 2^k - 2$ and, knowing M_1 we can find M_3. Finally, the last remaining unknown M_0 can be evaluated from the obvious equation $M_0 + M_1 + M_3 = |\mathrm{GF}(2^k)^*| = 2^k - 1$.□

Note that Bluher in [5, Theorem 5.6] (see Theorem 2 below), in particular, found the possible number of zeros of $P_a(x)$ and calculated the corresponding values of M_i, in the notations of our Theorem 1. This was also done earlier for odd k in [11, Lemma 9].

4. Zeros of $P_a(x)$ when $\gcd(l,k) \geq 1$

In this section, we analyze the zeros in $\mathrm{GF}(2^k)$ of the polynomial $P_a(x)$ assuming that l, k are positive integers with $l < k$ and $\gcd(l,k) = d \geq 1$. In this case, let $k = nd$ for some $n > 1$ and also recall our notation $u_i = u^{2^{il}}$ for any $u \in \mathrm{GF}(2^k)$ and $i = 0, \ldots, n-1$. First, keep in mind the following result that can be obtained combining Theorems 5.6 and 6.4 in [5].

Theorem 2 ([5]) *For any $b \in \mathrm{GF}(2^k)^*$, take polynomials*

$$f(x) = x^{2^l+1} + b^2 x + b^2 \quad \textit{and} \quad g(x) = b^{-1} f(bx^{2^l-1}) = b^{2^l} x^{2^{2l}-1} + b^2 x^{2^l-1} + b$$

over $\mathrm{GF}(2^k)$ and let $\gcd(l,k) = d$. Then exactly one of the following holds

(i) *$f(x)$ has none or two zeros in $\mathrm{GF}(2^k)$ and $g(x)$ has none zeros in $\mathrm{GF}(2^k)$;*

(ii) *$f(x)$ has one zero in $\mathrm{GF}(2^k)$, $g(x)$ has $2^d - 1$ zeros in $\mathrm{GF}(2^k)$ and each rational root δ of $g(x)$ satisfies $\mathrm{Tr}_d^k\left(b^{-1}\delta^{-(2^l+1)}\right) \neq 0$;*

(iii) *$f(x)$ has $2^d + 1$ zeros in $\mathrm{GF}(2^k)$, $g(x)$ has $2^{2d} - 1$ zeros in $\mathrm{GF}(2^k)$ and each rational root δ of $g(x)$ satisfies $\mathrm{Tr}_d^k\left(b^{-1}\delta^{-(2^l+1)}\right) = 0$.*

Let T_i denote the number of $b \in \mathrm{GF}(2^k)^*$ such that $f(x) = 0$ has exactly i roots in $\mathrm{GF}(2^k)$. Then the following distribution holds for k/d odd (resp. k/d even)

$$\begin{array}{lcll} T_0 & = & \frac{(2^k+1)2^{d-1}}{2^d+1} & (\textit{resp. } \frac{(2^k-1)2^{d-1}}{2^d+1}) \ , \\ T_1 & = & 2^{k-d} - 1 & (\textit{resp. } 2^{k-d}) \ , \\ T_2 & = & \frac{(2^k-1)(2^{d-1}-1)}{2^d-1} & (\textit{in both cases}) \ , \\ T_{2^d+1} & = & \frac{2^{k-d}-1}{2^{2d}-1} & (\textit{resp. } \frac{2^{k-d}-2^d}{2^{2d}-1}) \ . \end{array}$$

Note 1. Take a linearized polynomial

$$L_a(x) = a^{2^l} x^{2^{2l}} + x^{2^l} + ax \ . \tag{20}$$

Note that zeros in $\mathrm{GF}(2^k)$ of $L_a(x)$ form a vector subspace over $\mathrm{GF}(2^d)$ and thus, the number of zeros can be equal to $1, 2^d, 2^{2d}, \ldots, 2^{2l}$ (we will see that, in fact, $L_a(x)$ can not have more than 2^{2d} zeros). Assume $a \neq 0$, then dividing $L_a(x)$ by $a_0 a_1 x$ (we remove one zero $x = 0$) and then substituting x with $a_0^{-1}x$ leads to $a_1^{-2^l} x^{2^{2l}-1} + a_1^{-2} x^{2^l-1} + a_1^{-1}$ which has the form of polynomial $g(x)$ from Theorem 2 taking $b = a_1^{-1}$ (note a 1-to-1 correspondence between a and b). This leads to the corresponding $f(x) = x^{2^l+1} + a_1^{-2}x + a_1^{-2}$. Finally, substituting x in the latter $f(x)$ with $a_0^{-2}x$ and multiplying by $a_0^2 a_1^2$ we get $x^{2^l+1} + x + a_0^2 = P_{a^2}(x)$. By Theorem 2, we obtain the relation between the number of zeros of $L_a(x)$ and $P_{a^2}(x)$. We also conclude that $P_a(x)$ has either 0, 1, 2 or $2^d + 1$ zeros in $\mathrm{GF}(2^k)$ and $M_i = T_i$ for $i = 0, 1, 2, 2^d + 1$. It can be checked directly that $L_a(x) = 0$ for some $x \neq 0$ if and only if $P_{a^2}(a_0 x^{2^l-1}) = 0$.

Proposition 2 *Take any $a \in \mathrm{GF}(2^k)^*$. Then polynomial $P_a(x)$ has none or exactly two zeros in $\mathrm{GF}(2^k)$ if and only if $Z_n(a) \neq 0$. Also if n is odd (resp. n is even) then*

$$\begin{array}{rcll} M_0 & = & \frac{(2^k+1)2^{d-1}}{2^d+1} & (\textit{resp. } \frac{(2^k-1)2^{d-1}}{2^d+1}) \ , \\ M_2 & = & \frac{(2^k-1)(2^{d-1}-1)}{2^d-1} & (\textit{in both cases}) \ . \end{array}$$

Proof. Consider the equation $L_a(x) = a_1 x_2 + x_1 + a_0 x_0 = 0$ and show that in our case, it has the only zero solution. Taking $L_a(x) = 0$ and all its 2^{il} powers we obtain n equations

$$L_a^{2^{il}}(x) = a_{i+1} x_{i+2} + x_{i+1} + a_i x_i = 0 \quad \text{for} \quad i = 0, \ldots, n-1 \ ,$$

where all indices are calculated modulo n. If x_i $(i = 0, \ldots, n-1)$ are considered as independent variables then the obtained system of n linear equations with n unknowns has the following matrix with the antidiagonal structure, assuming $n > 2$

$$\begin{pmatrix} 0 & 0 & \cdots & a_1 & 1 & a_0 \\ 0 & & \iddots & 1 & a_1 & 0 \\ \vdots & \iddots & \iddots & \iddots & & \vdots \\ a_{n-2} & 1 & \iddots & \iddots & & 0 \\ 1 & a_{n-2} & & & 0 & a_{n-1} \\ a_{n-1} & 0 & \cdots & 0 & a_0 & 1 \end{pmatrix} . \tag{21}$$

If $n = 2$ then $l = d$ and $L_a(x) = x_1 + (a_0 + a_1)x_0$. The corresponding matrix is $\mathcal{M}_2 = \begin{pmatrix} 1 & a_0 + a_1 \\ a_0 + a_1 & 1 \end{pmatrix}$ having the determinant equal to

$$1 + a_0^2 + a_1^2 = Z_2^2(a) \neq 0 \ .$$

Let the columns of (21) be numbered from 1 to $n > 2$. Permuting the columns in (21) (reorder them as $n-1, n-2, \ldots, 1, n$) we obtain a symmetric three-diagonal cyclic matrix $\mathcal{M}_n$ containing ones on the main diagonal, with

$$\mathcal{M}_n(i, i+1) = \mathcal{M}_n(i+1, i) = a_i \quad \text{for} \quad i = 1, \ldots, n-1$$

and corner elements $\mathcal{M}_n(1, n) = \mathcal{M}_n(n, 1) = a_0$. If $\boldsymbol{x} = (x_1, \ldots, x_{n-1}, x_0)^{\mathrm{T}}$ and $\mathbf{0} = (0, \ldots, 0)^{\mathrm{T}}$ then the system has the following matrix representation

$$\mathcal{M}_n \boldsymbol{x} = \mathbf{0} \ . \tag{22}$$

The determinant of (21) is equal to the determinant of $\mathcal{M}_n$ and can be computed expanding the latter by minors along the last row. Doing this it is easy to see that

$$\begin{aligned}
\det \mathcal{M}_n \quad &= \quad \Delta_a(1, n-2) + a_{n-1}(a_{n-1}\Delta_a(1, n-3) + a_0 \ldots a_{n-2}) \\
&\qquad + a_0(a_0 \Delta_a(2, n-2) + a_1 \ldots a_{n-1}) \\
&\overset{(12,13)}{=} C_n^2(a) + a_{n-1}^2 C_{n-1}^2(a) + (a_0 C_{n-1}^{2^l}(a))^2 \\
&\overset{(4)}{=} C_{n+1}^2(a) + (a_0 C_{n-1}^{2^l}(a))^2 \\
&\overset{(7)}{=} Z_n^2(a) \neq 0 \ .
\end{aligned}$$

Thus, (22) has exactly one solution which is $\boldsymbol{x} = \mathbf{0}$. Now note that every $x \in \mathrm{GF}(2^k)$ with $L_a(x) = 0$ provides a solution to the system given by $x_i = x^{2^{il}}$ for $i = 0, \ldots, n-1$. Therefore, if $Z_n(a) \neq 0$ then $L_a(x) = 0$ has exactly one root (which is equal to zero). By Note 1 and Theorem 2 (i), $P_{a^2}(x)$ has either none or exactly two zeros in $\mathrm{GF}(2^k)$ and the identities for M_0 and M_2 follow as well. Finally, note that $Z_n(a^2) = Z_n^2(a)$ and, therefore, the conditions of the theorem are satisfied by any a^{2^i} with $i = 0, \ldots, k-1$.

Using Corollary 1, we can obtain the number of $a \in \mathrm{GF}(2^k)^*$ such that $Z_n(a) \neq 0$ (note that $Z_n(0) = 1$). Observe that this number is identical to $T_0 + T_2$ taken from Theorem 2 that is equal to the number of $a \in \mathrm{GF}(2^k)^*$ such that $P_a(x) = 0$ has none or exactly two roots in $\mathrm{GF}(2^k)$ (see Note 1). Therefore, if $P_a(x)$ has none or exactly two roots in $\mathrm{GF}(2^k)$ then a is necessarily such that $Z_n(a) \neq 0$. □

The following proposition provides a criterion to distinguish between the cases when $P_a(x)$ has none and when it has exactly two zeros in $\mathrm{GF}(2^k)$.

Proposition 3 *Take any $a \in \mathrm{GF}(2^k)^*$. Then polynomial $P_a(x)$ has exactly two zeros in $\mathrm{GF}(2^k)$ if and only if $Z_n(a) \neq 0$ and $\mathrm{Tr}_d\left(\mathrm{N}_d^k(a)/Z_n^2(a)\right) = 0$. Moreover, if d is odd then these two zeros are $(W+\mu)Z_n(a)/C_n(a)$ for $\mu \in \{0,1\}$, where*

$$W = \frac{C_{n+1}(a)}{Z_n(a)} + \sum_{i=0}^{\frac{d-1}{2}} \left(\frac{\mathrm{N}_d^k(a)}{Z_n^2(a)}\right)^{2^{2i}} .$$

Proof. First, consider equation $a^{2^l}x^{2^l+1} + x + a = 0$. Using the substitution $x = a^{-1}y$ and multiplying by a, the latter equation is transformed into $P_{a^2}(y) = y^{2^l+1} + y + a^2 = 0$ having the same number of roots. Thus, by Proposition 2, $a^{2^l}x^{2^l+1} + x + a$ has none or exactly two zeros if and only if $Z_n(a^2) = Z_n^2(a) \neq 0$.

We prove by induction that for any $u \in \mathrm{GF}(2^k)$ being a root of this equation and $i = 1, \ldots, n$ holds

$$u_i = \frac{uC_{i+1}^2(a) + a(C_i^2(a))^{2^l}}{a_i\left(uC_i^2(a) + a(C_{i-1}^2(a))^{2^l}\right)}$$

assuming $C_0(x) = 0$. For $i = 1$ the identity is obvious since $a_1u^{2^l+1}+u+a = 0$. Assuming the identity holds for $i < t$ we get for $i = t > 1$

$$\begin{aligned} u_t = u_{t-1}^{2^l} &= \frac{u_1(C_t^2(a))^{2^l} + a_1(C_{t-1}^2(a))^{2^{2l}}}{a_t\left(u_1(C_{t-1}^2(a))^{2^l} + a_1(C_{t-2}^2(a))^{2^{2l}}\right)} \\ &= \frac{(u+a)(C_t^2(a))^{2^l} + ua_1^2(C_{t-1}^2(a))^{2^{2l}}}{a_t\left((u+a)(C_{t-1}^2(a))^{2^l} + ua_1^2(C_{t-2}^2(a))^{2^{2l}}\right)} \\ &\overset{(5)}{=} \frac{uC_{t+1}^2(a) + a(C_t^2(a))^{2^l}}{a_t\left(uC_t^2(a) + a(C_{i-1}^2(a))^{2^l}\right)} \end{aligned}$$

using induction hypothesis and since $u_1 = (u+a)/a_1u$.

In particular, for $i = n$ we get

$$u_n = u = \frac{uC_{n+1}^2(a) + a(C_n^2(a))^{2^l}}{a\left(uC_n^2(a) + a(C_{n-1}^2(a))^{2^l}\right)} \quad \text{and}$$

$$aC_n^2(a)u^2 + \left(C_{n+1}(a) + aC_{n-1}^{2^l}(a)\right)^2 u \overset{(7)}{=} aC_n^2(a)u^2 + Z_n^2(a)u = a\left(C_n^2(a)\right)^{2^l} .$$

Note that the latter equation is a trivial identity when $C_n(a) = 0$, i.e., when $P_a(y)$ has more than two zeros (see Proposition 5). Now use the substitution $u = vZ_n^2(a)/aC_n^2(a)$ to obtain $v^2 + v = \left(aC_n^{2^l+1}(a)/Z_n^2(a)\right)^2$ (obviously, $C_n(a) \neq 0$ when $Z_n(a) \neq 0$). Observe that

$$\frac{aC_n^{2^l+1}(a)}{Z_n^2(a)} \overset{(6)}{=} \frac{aC_{n-1}^{2^l}(a)C_{n+1}(a)}{Z_n^2(a)} + \frac{\mathrm{N}_d^k(a)}{Z_n^2(a)} \overset{(7)}{=} \frac{C_{n+1}(a)}{Z_n(a)} + \frac{C_{n+1}^2(a)}{Z_n^2(a)} + \frac{\mathrm{N}_d^k(a)}{Z_n^2(a)} \quad (23)$$

and thus, $\mathrm{Tr}_k\left(aC_n^{2^l+1}(a)/Z_n^2(a)\right) = n\mathrm{Tr}_d\left(\mathrm{N}_d^k(a)/Z_n^2(a)\right)$ since $Z_n(a) \in \mathrm{GF}(2^d)$. Therefore, if n is odd and $a^{2^l}x^{2^l+1}+x+a = 0$ has exactly two roots in $\mathrm{GF}(2^k)$ then $Z_n(a) \neq 0$ and $\mathrm{Tr}_d\left(\mathrm{N}_d^k(a)/Z_n^2(a)\right) = 0$.

For the case when n is even, some additional arguments are needed. Note that

$$\left(\frac{\mathrm{N}_d^k(a)}{Z_n^2(a)}\right)^2 \overset{(23)}{=} \left(v + \frac{C_{n+1}^2(a)}{Z_n^2(a)}\right) + \left(v + \frac{C_{n+1}^2(a)}{Z_n^2(a)}\right)^2 \quad \text{and}$$

$$\left(v + \frac{C_{n+1}^2(a)}{Z_n^2(a)}\right)^{2^l} = \left(\frac{aC_n^{2^l+1}(a)}{Z_n^2(a)}\right)^2 v^{-1} + \frac{(C_n^2(a))^{2^l} + (C_{n+1}^2(a))^{2^l}}{Z_n^2(a)}$$

$$\overset{(4)}{=} v + 1 + \frac{a^2(C_{n-1}^2(a))^{2^l}}{Z_n^2(a)} \overset{(7)}{=} v + \frac{C_{n+1}^2(a)}{Z_n^2(a)}$$

since $a^{2^l}u^{2^l+1} + u + a = 0$ and using the relation between u and v. Thus, $v + \frac{C_{n+1}^2(a)}{Z_n^2(a)} \in \mathrm{GF}(2^d)$ and $\mathrm{Tr}_d\left(\mathrm{N}_d^k(a)/Z_n^2(a)\right) = 0$.

Now prove the converse implication. Take an arbitrary n and assume $Z_n(a) \neq 0$ and $\mathrm{Tr}_d\left(\mathrm{N}_d^k(a)/Z_n^2(a)\right) = 0$. Since $\mathrm{Tr}_k\left(aC_n^{2^l+1}(a)/Z_n^2(a)\right) = 0$ there exists some $v \in \mathrm{GF}(2^k)$ with $v^2 + v = \left(aC_n^{2^l+1}(a)/Z_n^2(a)\right)^2$. Using the substitution $u = vZ_n^2(a)/aC_n^2(a)$ we also obtain $aC_n^2(a)u^2 + Z_n^2(a)u = a(C_n^2(a))^{2^l}$. It is easy to see that

$$v^{2^l} + v = \sum_{i=1}^{l}\left(\frac{aC_n^{2^l+1}(a)}{Z_n^2(a)}\right)^{2^i}$$

$$\overset{(23)}{=} \frac{C_{n+1}^2(a)}{Z_n^2(a)} + \frac{(C_{n+1}^{2^l}(a))^2}{Z_n^2(a)} + \frac{l}{d}\mathrm{Tr}_d\left(\frac{\mathrm{N}_d^k(a)}{Z_n^2(a)}\right)$$

$$\overset{(4,7)}{=} \frac{(C_n^{2^l}(a) + Z_n(a))^2}{Z_n^2(a)} = \frac{(C_n^{2^l}(a))^2}{Z_n^2(a)} + 1 \ .$$

Note that n and l/d can not be even together. Using the substitution $u = vZ_n^2(a)/aC_n^2(a)$ we obtain

$$\begin{aligned} \left(aC_n^2(a)\right)^{2^l} u^{2^l} + aC_n^2(a)u &= \left(C_n^{2^l}(a)\right)^2 + Z_n^2(a) \quad \text{and} \\ \left(aC_n^2(a)\right)^{2^l} u^{2^l+1} + Z_n^2(a)u + a\left(C_n^2(a)\right)^{2^l} &= u\left(\left(C_n^{2^l}(a)\right)^2 + Z_n^2(a)\right) \end{aligned}$$

which gives $a^{2^l}u^{2^l+1} + u = a$. Thus, $P_a(x)$ has a zero and, by Proposition 2, it has exactly two zeros.

Finally, note that the solution in $\mathrm{GF}(2^d)$ of the equation $x^2 + x = u$ for some $u \in \mathrm{GF}(2^d)$ with $\mathrm{Tr}_d(u) = 0$ and odd d can be written as $\sum_{i=0}^{\frac{d-1}{2}} u^{2^{2i}}$ or $\sum_{i=0}^{\frac{d-3}{2}} u^{2^{2i+1}}$. This way we obtain $v = W^2+\mu$ thus, $u = (W^2+\mu)Z_n^2(a)/aC_n^2(a)$ and $P_{a^2}((W^2 + \mu)Z_n^2(a)/C_n^2(a)) = 0$ for $\mu \in \{0, 1\}$. It is also not difficult to check by the direct calculations that $P_a((W + \mu)Z_n(a)/C_n(a)) = 0$ if $\mathrm{Tr}_d\left(\mathrm{N}_d^k(a)/Z_n^2(a)\right) = 0$. □

In the case when $d = 1$, if $Z_n(a) \neq 0$ (i.e., $Z_n(a) = 1$) then $\mathrm{Tr}_d\left(\mathrm{N}_d^k(a)/Z_n^2(a)\right) = 0$ only for $a = 0$ and thus, $P_a(x)$ has two zeros in $\mathrm{GF}(2^k)$ only for $a = 0$. The next proposition follows from Propositions 2 and 5. We provide this proof yet, independently of previous statements, since its major part contains the result needed for proving the fact from Corollary 1 and for the sake of giving the complete picture of the addressed problem.

Proposition 4 *Take any $a \in \mathrm{GF}(2^k)^*$. Then polynomial $P_a(x)$ has exactly one zero in $\mathrm{GF}(2^k)$ if and only if $Z_n(a) = 0$ and $C_n(a) \neq 0$. Moreover, this zero is equal to $\left(aC_n^{2^l-1}(a)\right)^{2^{k-1}}$ and if n is odd (resp. n is even) then*

$$M_1 = 2^{k-d} - 1 \quad (\textit{resp. } 2^{k-d}) \ .$$

Proof. Note that without loss of generality, we can substitute a with a^2 in the claimed result. First, assume $Z_n(a) = 0$ and $C_n(a) \neq 0$ (equivalently, we can take a^2). Now we find the number of zeros of $L_a(x)$ in $\mathrm{GF}(2^k)$. Note

that

$$\begin{aligned} L_a(C_n(a)) &= a_1 C_n^{2^{2l}}(a) + C_n^{2^l}(a) + a_0 C_n(a) \\ &\overset{(4)}{=} a_1 C_{n-1}^{2^{2l}}(a) + a_1 a_0 C_{n-2}^{2^{2l}}(a) + C_n^{2^l}(a) + a_0 C_n(a) \\ &\overset{(5)}{=} C_{n+1}(a) + a_0 C_{n-1}^{2^l}(a) \\ &\overset{(7)}{=} Z_n(a) = 0 \ . \end{aligned}$$

Therefore, if $C_n(a) \neq 0$ then 2^d distinct elements $\mu C_n(a) \in \mathrm{GF}(2^k)$ for $\mu \in \mathrm{GF}(2^d)$ are also zeros of $L_a(x)$ (since $\mathrm{GF}(2^k) \bigcap \mathrm{GF}(2^l) = \mathrm{GF}(2^d)$).

It is not difficult to see that in our case, $L_a(x)$ can not have more than 2^d zeros in $\mathrm{GF}(2^k)$. Indeed, consider matrix $\mathcal{M}_n$ of the system of n linear equations (22). Note that $\det \mathcal{M}_n = Z_n^2(a) = 0$ and a principal submatrix obtained by deleting the last column and the last row from $\mathcal{M}_n$ is nonsingular with the determinant $\Delta_a(1, n-2) = C_n^2(a) \neq 0$ (see (12)). Therefore, applying equivalent row transformations to $\mathcal{M}_n$ we can obtain a matrix containing a nonsingular diagonal submatrix lying in the first $n-1$ columns and rows. Thus, the equation given by one of the first $n-1$ rows (take row $i \in \{1, \ldots, n-1\}$ with $il \equiv d \pmod{k}$) of this equivalent matrix is nonzero and has degree 2^d. We conclude that system (22) can not have more than 2^d solutions and the same holds for the equation $L_a(x) = 0$. Note that on the side, we have found a factor $x^{2^d} + C_n^{2^d-1}(a)x$ of $L_a(x)$ that contains all its zeros in $\mathrm{GF}(2^k)$.

By Note 1 and Theorem 2 (ii), $P_{a^2}(x)$ has exactly one zero in $\mathrm{GF}(2^k)$ that is equal to $a(\mu C_n(a))^{2^l-1} = aC_n^{2^l-1}(a)$ and the identities for M_1 follow as well.

Now we prove the converse implication. Assume $P_{a^2}(x)$ has exactly one zero in $\mathrm{GF}(2^k)$. Here we use the technique found by Bluher [5] for counting the number of $b \in \mathrm{GF}(2^k)^*$ for which $f_b(y) = y^{2^l+1} + by + b$ has exactly one zero in $\mathrm{GF}(2^k)$. For any $v \in S$ with S coming from (10) define $r = v^{1-2^l} + 1 \in \mathrm{GF}(2^k) \setminus \{0, 1\}$ and corresponding $b = \frac{r^{2^l+1}}{r+1} \neq 0$. Obviously, such an r is a zero of $f_b(y)$. Note that

$$b = \frac{r^{2^l+1}}{r+1} = v^{2^l-1}(v^{1-2^l}+1)^{2^l+1} = \frac{(v+v^{2^l})^{2^l+1}}{v^{2^{2l}+1}} = V^{-1} \ , \qquad (24)$$

where V comes from (8). Then, by Proposition 1 and Corollary 1, $C_n(b^{-1}) \neq 0$ and $Z_n(b^{-1}) = 0$. By the implication already proved, $P_{b^{-1}}(x)$ has exactly

one zero in $\mathrm{GF}(2^k)$. After substituting x in the latter polynomial with $b^{-1}y$, we get polynomial $f_{b^{2^l}}(y)$ having the same number of zeros as $P_{b^{-1}}(x)$. Thus, $f_b(y)$ (as well as $f_{b^{2^l}}(y)$) has exactly one zero in $\mathrm{GF}(2^k)$.

Now we prove that function (24) that maps every $v \in S$ to $b \in \mathrm{GF}(2^k)^*$ is a (2^d-1)-to-1 mapping. First, note that (2^l-1)-power is a (2^d-1)-to-1 mapping of S to $\mathrm{GF}(2^k)^*$. Indeed, if $x \in S$ and $x^{2^l-1} = t$ then the latter identity holds for all distinct $\delta x \in S$ with $\delta \in \mathrm{GF}(2^d)^*$ since $\mathrm{Tr}_d^k(\delta x) = \delta \mathrm{Tr}_d^k(x) \neq 0$ and $\delta x \notin \mathrm{GF}(2^d)$. Thus, every $r = v^{1-2^l} + 1$ is obtained from $2^d - 1$ different values of v. Finally, the mapping from r to b is 1-to-1 since for the obtained b the equation $f_b(y) = 0$ has exactly one root r.

Therefore, taking all $v \in S$ and using (24), we obtain $|S|/(2^d-1)$ different values of $b \in \mathrm{GF}(2^k)^*$ and this number is equal to the total number of b such that $f_b(y)$ has exactly one zero (see Theorem 2). Therefore, these and only these values of b satisfying (24) result in the polynomials $f_b(y)$ having exactly one zero.

After substituting x in $P_{a^2}(x)$ with a^2y, we get polynomial $f_b(y)$ with $b = a^{-2^{l+1}}$ having the same number of zeros as $P_{a^2}(x)$. If polynomial $P_{a^2}(x)$ has exactly one zero then $f_b(y)$ also has exactly one zero and, thus, b is obtained by (24). Therefore, by Proposition 1, $C_n(b^{-1}) = C_n(a^{2^{l+1}}) = C_n(a^2)^{2^l} \neq 0$ and, thus, $C_n(a^2) \neq 0$. Also, by Corollary 1, $Z_n(a^2) = 0$. □

Note that if $Z_n(a) = 0$ and $C_n(a) \neq 0$ then, by Proposition 1 and Corollary 1, a has the form of (8) for some $v \in \mathrm{GF}(2^k) \setminus \mathrm{GF}(2^d)$ with $\mathrm{Tr}_d^k(v) \neq 0$ and

$$\begin{aligned} aC_n^{2^l+1}(a) &= \mathrm{Tr}_d^k(v)^2 \mathrm{N}_d^k\left(\frac{v}{v+v^{2^l}}\right)^2 v^{-2^{l+1}} \qquad \text{so} \\ \mathrm{Tr}_d^k\left(a^{-1}C_n^{-(2^l+1)}(a)\right) &= \mathrm{N}_d^k\left(1+v^{2^l-1}\right)^2 \neq 0 \ . \end{aligned}$$

This complies with the trace property from Theorem 2 (ii). Indeed, take $b = a_1^{-1}$ and $\delta = \mu a C_n(a)$ for any $\mu \in \mathrm{GF}(2^d)^*$ then $g(\delta) = \frac{L_a(C_n(a))}{a^{2^l+1}C_n(a)} = 0$ and $b^{-1}\delta^{-(2^l+1)} = \mu^{-2}a^{-1}C_n^{-(2^l+1)}(a)$.

Now we are left with the remaining case when $C_n(a) = 0$ (then, by Corollary 1, $Z_n(a) = 0$). The next proposition follows from Propositions 2 and 4. We provide this proof yet, independently of previous statements, since its major part contains the result used for proving the converse implication and also needed for proving the fact from Proposition 1. It is also worth mentioning [2, Lemma 22], where the authors found an interesting parametrization

for the set containing all 2^d+1 zeros of $x^{2^l+1}+ax^{2^l}+bx+c$ in $\mathrm{GF}(2^k)$. The latter polynomial is directly related to $P_a(x)$, as noted in the introduction.

Proposition 5 *Take any $a \in \mathrm{GF}(2^k)^*$. Then polynomial $P_a(x)$ has exactly 2^d+1 zeros in $\mathrm{GF}(2^k)$ if and only if $C_n(a)=0$. Also if n is odd (resp. n is even) then*

$$M_{2^d+1} = \frac{2^{k-d}-1}{2^{2d}-1} \quad (\textit{resp. } \frac{2^{k-d}-2^d}{2^{2d}-1}) \ .$$

Proof. Here we use the technique found by Bluher [5] for counting the number of $b \in \mathrm{GF}(2^k)^*$ for which $f_b(y) = y^{2^l+1}+by+b$ has 2^d+1 zeros in $\mathrm{GF}(2^k)$. Denote $G = \mathrm{GF}(2^k) \setminus \mathrm{GF}(2^{2d})$ and observe that

$$\mathrm{GF}(2^k) \cap \mathrm{GF}(2^{2l}) = \mathrm{GF}(2^{d\gcd(n,2)}) \subseteq \mathrm{GF}(2^{2d}) \ .$$

Therefore, taking any $u \in \mathrm{GF}(2^k)$ such that $u \notin \mathrm{GF}(2^{2d})$ implies $u^{2^{2l}} \neq u$ and $(u+u^{2^l})^{2^l} \neq u+u^{2^l}$ or, equivalently, $u+u^{2^l} \notin \mathrm{GF}(2^l)$ which is the same as $u+u^{2^l} \notin \mathrm{GF}(2^d)$. Now we can define $r = (u+u^{2^l})^{1-2^l}+1 \in \mathrm{GF}(2^k) \setminus \{0,1\}$ and corresponding $b = \frac{r^{2^l+1}}{r+1} \neq 0$. Obviously, such an r is a zero of $f_b(y)$. Define also $r_0 = ru^{2^l-1}$ and $r_1 = r(u+1)^{2^l-1}$ and note that r, r_0 and r_1 are pairwise distinct. Further,

$$f_b(r_0) = r^{2^l+1}u^{2^{2l}-1} + bru^{2^l-1} + b = b((r+1)u^{2^{2l}} + ru^{2^l} + u)/u = 0$$

since $r(u+u^{2^l})^{2^l} = u+u^{2^{2l}}$ by the definition of r. Also, similarly, we get

$$f_b(r_1) = \frac{b((r+1)(u+1)^{2^{2l}} + r(u+1)^{2^l} + (u+1))}{u+1} = \frac{b(r+1+r+1)}{u+1} = 0 \ .$$

Thus, $f_b(y)$ with such a b has at least three zeros and, by Theorem 2, it has 2^d+1 zeros. Note that

$$b = \frac{r^{2^l+1}}{r+1} = (u+u^{2^l})^{2^l-1}((u+u^{2^l})^{1-2^l}+1)^{2^l+1} = \frac{(u+u^{2^{2l}})^{2^l+1}}{(u+u^{2^l})^{2^{2l}+1}} = V^{-1} \ , \quad (25)$$

where V comes from (8) assuming $v = u+u^{2^l}$.

Now we prove that function (25) that maps every $u \in G$ to $b \in \mathrm{GF}(2^k)^*$ is a $(2^{3d}-2^d)$-to-1 mapping. First, note that $u \mapsto u+u^{2^l}$ is a 2^d-to-1 mapping onto

$$F = \{x \in \mathrm{GF}(2^k) \setminus \mathrm{GF}(2^d) \mid \mathrm{Tr}_d^k(x) = 0\}$$

(see explanations in the proof of Proposition 1). Further, (2^l-1)-power is a (2^d-1)-to-1 mapping of F to $\mathrm{GF}(2^k)^*$. Indeed, if $x \in F$ and $x^{2^l-1} = t$ then the latter identity holds for all distinct $\delta x \in F$ with $\delta \in \mathrm{GF}(2^d)^*$ since $\mathrm{Tr}_d^k(\delta x) = \delta \mathrm{Tr}_d^k(x) = 0$ and $\delta x \notin \mathrm{GF}(2^d)$. Thus, every $r = (u+u^{2^l})^{1-2^l}+1$ is obtained from $2^d(2^d-1)$ different values of u. Finally, the mapping from r to b is (2^d+1)-to-1 since for the obtained b the equation $f_b(y) = 0$ has (2^d+1) roots and every root r satisfies $(r+1)^{-1} \in F^{2^l-1}$. Indeed, let r, r_0 and r_1 be any distinct zeros of $f_b(y)$ (not necessarily the ones defined above) and define $u = (r+r_1)/(r_0+r_1)$. Note that

$$rr_0(r+r_0)^{2^l} = r_0 r^{2^l+1} + r r_0^{2^l+1} = r_0 b(r+1) + rb(r_0+1) = b(r+r_0)$$

and so $b = rr_0(r+r_0)^{2^l-1} = rr_1(r+r_1)^{2^l-1} = r_0 r_1 (r_0+r_1)^{2^l-1}$. Then

$$u^{2^{2l}-1} = (r_0/r)^{2^l+1} = (r_0+1)/(r+1) \neq 1$$

and, thus, $u \in G$. The identity $(r+1)^{-1} = (u+u^{2^l})^{2^l-1} \in F^{2^l-1}$ follows from [5, Lemma 2.1].

Therefore, taking all $u \in G$ and using (25), we obtain $|G|/(2^{3d}-2^d)$ different values of $b \in \mathrm{GF}(2^k)^*$ and this number is equal to the total number of b such that $f_b(y)$ has 2^d+1 zeros (see Theorem 2). Therefore, these and only these values of b satisfying (25) result in the polynomials $f_b(y)$ having 2^d+1 zeros.

Now note that without loss of generality, we can put a^2 in place of a in the result we are claiming. Then, after substituting x in $P_{a^2}(x)$ with $a^2 y$, we get polynomial $f_b(y)$ with $b = a^{-2^{l+1}}$ having the same number of zeros as $P_{a^2}(x)$. In particular, polynomial $P_{a^2}(x)$ has exactly 2^d+1 zeros in $\mathrm{GF}(2^k)$ if and only if the same holds for the corresponding polynomial $f_b(y)$ and this is equivalent to b having the form of (25). It remains to apply Proposition 1 and note that $C_n(b^{-1}) = C_n(a^{2^{l+1}}) = C_n^{2^l}(a^2)$ and the latter is equal to zero if and only if $C_n(a^2) = 0$. The identities for M_{2^d+1} follow from Note 1 and Theorem 2 (iii). $\square$

Note that if $Z_n(a) = 0$ then, by Corollary 1, a has the form of (8) for some $v \in \mathrm{GF}(2^k) \backslash \mathrm{GF}(2^d)$ and it is straightforward to check that $P_a\left(v/(v+v^{2^l})\right) = 0$. This also complies with Proposition 4 since if, additionally, $C_n(a) \neq 0$ then, by (9), $\left(aC_n^{2^l-1}(a)\right)^{2^{k-1}} = v/(v+v^{2^l})$. The following corollary follows by combining Theorem 1 and Proposition 4.

Corollary 4 *Take any* $a \in \mathrm{GF}(2^k)^*$ *and positive integer* $l < k$ *with* $\gcd(l,k) = 1$. *Then* $\mathrm{Tr}_k(R(a^{-1})+1) = 1$ *if and only if* $Z_k(a) = 0$ *and* $C_k(a) \neq 0$, *where* $R(x)$, $C_k(x)$ *and* $Z_k(x)$ *are defined in (2), (4) and (7) respectively.*

5. Related Affine Polynomial

In this section, we consider zeros in $\mathrm{GF}(2^k)$ of the affine polynomial $F_a(x)$ defined in (1). Obviously, either $F_a(x)$ has no zeros in $\mathrm{GF}(2^k)$ or it has exactly the same number of zeros as its linearized homogeneous part $L_a(x)$ defined in (20). It was shown in Note 1 that $L_a(x)/x$ and polynomial $g(x)$ from Theorem 2 are related by a one-to-one substitution of variable. On the other hand, $P_a(x)$ and polynomial $f(x)$ from the same theorem are related in a similar way. Thus, we can use Theorem 2 and the results from the previous sections to analyze the number of zeros of $F_a(x)$ if we show that is has at least one zero in $\mathrm{GF}(2^k)$. Moreover, since $L_a(cv) = cL_a(v)$ for any $v \in \mathrm{GF}(2^k)$ and $c \in \mathrm{GF}(2^d)$, where $d = \gcd(l,k)$, we can equivalently assume

$$F_a(x) = a^{2^l} x^{2^{2l}} + x^{2^l} + ax + c \ .$$

We know already from Lemma 2 that if $d = 1$ and $a \neq 0$ then $cR(a^{-1})$, where $R(x)$ comes from (2), is a zero of $F_a(x)$. Recall the notation $n = k/d$ and let also

$$N_i = \{a \mid a \in \mathrm{GF}(2^k)^* \text{ and } F_a(x) \text{ has exactly } i \text{ zeros in } \mathrm{GF}(2^k)\} \ .$$

Lemma 5 *Take any* $a \in \mathrm{GF}(2^k)^*$ *and assume* $F_a(x)$ *has a zero in* $\mathrm{GF}(2^k)$, *say* $F_a(\mathcal{V}) = 0$. *Then for any* $v \in \mathrm{GF}(2^k)$ *with* $F_a(v) = 0$ *holds*

$$\mathrm{Tr}_d^k(v) = \mathrm{Tr}_d^k(\mathcal{V}) \in \{0, c\} \ .$$

Moreover, if $d = 1$ *then*

$$\begin{aligned} \mathrm{Tr}_k(av^{2^l+1}) &= l'\mathrm{Tr}_k(R(a^{-1})) + \mathrm{Tr}_k(l'+1), \qquad \text{if} \quad v = R(a^{-1}) \\ &= l'\mathrm{Tr}_k(R(a^{-1})) + \mathrm{Tr}_k(l'), \qquad \text{if} \quad v \neq R(a^{-1}) \ , \end{aligned}$$

where $R(x)$ *is defined in (2) and* $l' = l^{-1} \pmod k$.

Proof. The first identity follows by observing that any zero of $F_a(x)$ is obtained as a sum of $\mathcal{V}$ and a zero of its homogeneous part $L_a(x)$. To prove

the identity it therefore suffices to show that $\mathrm{Tr}_d^k(u) = 0$ for any u with $a^{2^l}u^{2^{2l}} + u^{2^l} + au = 0$. This follows from

$$\mathrm{Tr}_d^k(u)^2 = \mathrm{Tr}_d^k(u^2) = \mathrm{Tr}_d^k(u^{2^{l+1}}) = \mathrm{Tr}_d^k(u^{2^l+2^l}) = \mathrm{Tr}_d^k(a^{2^l}u^{2^{2l}+2^l} + au^{2^l+1}) = 0$$

and thus, $\mathrm{Tr}_d^k(u) = 0$ as claimed. Also similarly, we get

$$\mathrm{Tr}_d^k(\mathcal{V})^2 = \mathrm{Tr}_d^k(\mathcal{V}^{2^l+2^l}) = \mathrm{Tr}_d^k(a^{2^l}\mathcal{V}^{2^{2l}+2^l} + a\mathcal{V}^{2^l+1} + c\mathcal{V}^{2^l}) = \mathrm{Tr}_d^k(c\mathcal{V}^{2^l}) = c\mathrm{Tr}_d^k(\mathcal{V})$$

which holds if and only if $\mathrm{Tr}_d^k(\mathcal{V}) \in \{0, c\}$.

Now assume $\gcd(l, k) = 1$ and let $\mathcal{V} = R(a^{-1})$ which, by Lemma 2, is a zero of $F_a(x)$ in $\mathrm{GF}(2^k)$. To prove the second identity for the case when $v = \mathcal{V}$, we use the fact presented in the proof of Lemma 2 that $a\mathcal{V}^{2^l+1} = \sum_{i=1}^{l'} \mathcal{V}^{2^{il}} + l' + 1$. Then $\mathrm{Tr}_k(a\mathcal{V}^{2^l+1}) = l'\mathrm{Tr}_k(\mathcal{V}) + \mathrm{Tr}_k(l' + 1)$.

Now note that since $F_a(v)$ is obtained by adding the 2^lth power of (14) to itself we have for $v \neq 0$

$$F_a(v) = 0 \quad \text{if and only if} \quad av^{2^l+1} + \sum_{i=1}^{l'} v^{2^{il}} + l' + 1 \in \{0, 1\} \ .$$

Since $\mathcal{V}$ is the only solution of (14), then for $v \neq \mathcal{V}$ with $F_a(v) = 0$ we have $av^{2^l+1} + \sum_{i=1}^{l'} v^{2^{il}} + l' + 1 = 1$ and

$$\mathrm{Tr}_k(av^{2^l+1}) = l'\mathrm{Tr}_k(v) + \mathrm{Tr}_k(l') = l'\mathrm{Tr}_k(\mathcal{V}) + \mathrm{Tr}_k(l')$$

using already proved identity that $\mathrm{Tr}_k(v) = \mathrm{Tr}_k(\mathcal{V})$. □

Proposition 6 *Take any $a \in \mathrm{GF}(2^k)$. Then polynomial $F_a(x)$ has exactly one zero in $\mathrm{GF}(2^k)$ if and only if $Z_n(a) \neq 0$. Moreover, this zero is equal to $\mathcal{V}_a = cC_n(a)/Z_n(a)$ and $\mathrm{Tr}_d^k(\mathcal{V}_a) = nc$. Also if n is odd (resp. n is even) then*

$$|N_1| = \frac{2^{k+2d} - 2^{k+d} - 2^k + 1}{2^{2d} - 1} \ (\textit{resp.} \ \frac{2^{k+2d} - 2^{k+d} - 2^k - 2^{2d} + 2^d + 1}{2^{2d} - 1}) \ .$$

Proof. Having Theorem 2 and Proposition 2, it suffices to show that $\mathcal{V}_a$ indeed is a zero of $F_a(x)$ if $Z_n(a) \neq 0$. First, recall that $Z_n(u) \in \mathrm{GF}(2^d)$ for any $u \in \mathrm{GF}(2^k)$. Therefore,

$$\begin{aligned} F_a(\mathcal{V}_a) &= \frac{c}{Z_n(a)}\Big(a_1C_n^{2^{2l}}(a) + C_n^{2^l}(a) + a_0C_n(a) + Z_n(a)\Big) \qquad (26) \\ &\overset{(4)}{=} \frac{c}{Z_n(a)}\Big(a_1C_{n-1}^{2^{2l}}(a) + a_1a_0C_{n-2}^{2^{2l}}(a) + C_n^{2^l}(a) + a_0C_n(a) + Z_n(a)\Big) \\ &\overset{(5)}{=} \frac{c}{Z_n(a)}\Big(C_{n+1}(a) + a_0C_{n-1}^{2^l}(a) + Z_n(a)\Big) = 0 \ . \end{aligned}$$

To prove the trace identity for $\mathcal{V}_a$ first note that for any $u \in \mathrm{GF}(2^k)$

$$\begin{aligned}\mathrm{Tr}_d^k(C_n(u)+Z_n(u)) &\overset{(7)}{=} \mathrm{Tr}_d^k\left(C_n(u)+C_{n+1}(u)+u_0C_{n-1}^{2^l}(u)\right)\\ &\overset{(4)}{=} \mathrm{Tr}_d^k\left(C_n(u)+C_n(u)+u_{n-1}C_{n-1}(u)+u_0C_{n-1}^{2^l}(u)\right)\\ &= \mathrm{Tr}_d^k\left(u_{n-1}C_{n-1}(u)+(u_{n-1}C_{n-1}(u))^{2^l}\right)=0\ .\end{aligned}$$

Therefore, since c and $Z_n(a)$ are both in $\mathrm{GF}(2^d)$, then

$$\mathrm{Tr}_d^k(\mathcal{V}_a)=\mathrm{Tr}_d^k\left(c+c\,\frac{C_n(a)+Z_n(a)}{Z_n(a)}\right)=nc+\frac{c}{Z_n(a)}\ \mathrm{Tr}_d^k(C_n(a)+Z_n(a))=nc\ .$$

Finally, $|N_1|=T_0+T_2$ taken from Theorem 2. □

Note that if $Z_n(a)\neq 0$ then, by Theorem 2 and Proposition 2, the linear operator $L_a(x)$ on $\mathrm{GF}(2^k)$ has the kernel of dimension zero and, thus, the number of elements in the image of L_a is 2^k. Thus, the equation $L_a(x)=c$ has a solution for any $c\in\mathrm{GF}(2^k)$ if $Z_n(a)\neq 0$. Also note that if $d=1$, $a\neq 0$ and $Z_k(a)\neq 0$, i.e., $Z_k(a)=1$, then, by Lemma 2, $R(a^{-1})=C_k(a)$.

Proposition 7 *Take any $a\in\mathrm{GF}(2^k)^*$. Then polynomial $F_a(x)$ has exactly 2^d zeros in $\mathrm{GF}(2^k)$ if and only if $Z_n(a)=0$ and $C_n(a)\neq 0$. In this case, $\mathrm{Tr}_d^k(v)=(n-1)c$ and, if n is even, then $\mathrm{Tr}_k\left(ac^{-2}v^{2^l+1}\right)$ is constant for any $v\in\mathrm{GF}(2^k)$ with $F_a(v)=0$. Moreover, if n is odd then these zeros are*

$$v_\mu=c\sum_{i=0}^{\frac{n-1}{2}}\frac{C_{n-1}^{2^{(2i+1)l}}(a)}{C_n^{2^{(2i+1)l}+2^{2il}-1}(a)}+\mu C_n(a)$$

for every $\mu\in\mathrm{GF}(2^d)$ and

$$\sum_{\mu\in\mathrm{GF}(2^d)}(-1)^{\mathrm{Tr}_k\left(ac^{-2}v_\mu^{2^l+1}\right)}=0\ .$$

Also if n is odd (resp. n is even) then $|N_{2^d}|=2^{k-d}-1$ (resp. 2^{k-d}).

PROOF. Having Theorem 2 and Proposition 4, it suffices to show that $F_a(x)$ has at least one zero in $\mathrm{GF}(2^k)$ if $Z_n(a) = 0$ and $C_n(a) \neq 0$. From now on assume $Z_n(a) = 0$, $C_n(a) \neq 0$. Note that in this case, by (26),

$$a_1 C_n^{2^{2l}}(a) + C_n^{2^l}(a) + a_0 C_n(a) = 0 \tag{27}$$

which means that all 2^d distinct elements $\mu C_n(a) \in \mathrm{GF}(2^k)$ for $\mu \in \mathrm{GF}(2^d)$ are zeros of $L_a(x)$, since $\mathrm{GF}(2^k) \bigcap \mathrm{GF}(2^l) = \mathrm{GF}(2^d)$.

Consider the following equation over $\mathrm{GF}(2^k)$

$$C_n(a)x^{2^l} + C_n^{2^l}(a)x = cC_{n-1}^{2^l}(a) \ . \tag{28}$$

Substituting $x = C_n(a)y$ we obtain

$$y^{2^l} + y = \frac{cC_{n-1}^{2^l}(a)}{C_n^{2^l+1}(a)}$$

which has a solution since, by Corollary 2, $\mathrm{Tr}_d^k\left(\frac{C_{n-1}^{2^l}(a)}{C_n^{2^l+1}(a)}\right) = 0$ (if $n > 2$) and $c \in \mathrm{GF}(2^d)$ (see explanations in the proof of Proposition 1).

Therefore, there exists some $u \in \mathrm{GF}(2^k)$ with

$$\begin{array}{rcrcl} C_n(a)u_1 & + & C_n^{2^l}(a)u_0 & = & cC_{n-1}^{2^l}(a) \quad \text{and} \\ C_n^{2^l}(a)u_2 + C_n^{2^{2l}}(a)u_1 & & & = & cC_{n-1}^{2^{2l}}(a) \ , \end{array}$$

where the second identity is obtained by raising the first one to the power of 2^l. Now, multiply the first identity by $a_0 C_n^{-2^l}(a)$, the second by $a_1 C_n^{-2^l}(a)$ and add them to obtain

$$\begin{aligned} & a_1u_2 + C_n^{-2^l}(a)\left(a_0C_n(a) + a_1C_n^{2^{2l}}(a)\right)u_1 + a_0u_0 \\ & \overset{(27)}{=} a_1u_2 + u_1 + a_0u_0 \\ & = cC_n^{-2^l}(a)\left(a_0C_{n-1}^{2^l}(a) + a_1C_{n-1}^{2^{2l}}(a)\right) \\ & \overset{(7)}{=} cC_n^{-2^l}(a)\left(a_0C_{n-1}^{2^l}(a) + C_{n+1}^{2^l}(a)\right) \overset{(4)}{=} c \ . \end{aligned}$$

Thus, $F_a(u) = 0$.

If $Z_n(a) = 0$ and $C_n(a) \neq 0$ then, by Proposition 1 and Corollary 1, $a = v_0^{2^{2l}+1}/(v_0+v_1)^{2^l+1}$ for some $v \in \mathrm{GF}(2^k) \setminus \mathrm{GF}(2^d)$ with $\mathrm{Tr}_d^k(v_0) \neq 0$. If $u \in \mathrm{GF}(2^k)$ is a solution of (28) then $F_a(u) = 0$ and, by (9),

$$\frac{v_2}{v_1+v_2}u_1 + \frac{v_0}{v_0+v_1}u_0 = c\frac{v_2+\cdots+v_n}{\mathrm{Tr}_d^k(v_0)} \ .$$

Taking the trace of the both sides, we get

$$\mathrm{Tr}_d^k\left(\frac{v_1}{v_0+v_1}u_0 + \frac{v_0}{v_0+v_1}u_0\right) = \mathrm{Tr}_d^k(u) = (n-1)c \ .$$

By Lemma 5, all zeros of $F_a(x)$ have the same trace in $\mathrm{GF}(2^d)$.

To prove the properties of $\mathrm{Tr}_k\left(ac^{-2}v^{2^l+1}\right)$, where $F_a(v) = 0$, we use the technique suggested by Dobbertin for proving [9, Theorem 1] (we did this already in the proof of Lemma 4). Assume $c = 1$. If $F_a(x)$ has 2^d zeros then, by Theorem 2, $P_a(x)$ has exactly one zero, say $x_0 \in \mathrm{GF}(2^k)$ with $x_0^{2^l+1} + x_0 = a$. Define polynomial $Q(x) = ax^{2^l} + x_0^2x + x_0$ and denote $\Gamma = x_0^{2^l-1} + x_0^{-1}$ (obviously $\Gamma \neq 0$ since $x_0 \neq 1$). As in Lemma 4, we can write $F_a(x) = Q(x)\left(Q(x)^{2^l-1} + \Gamma\right)$.

Since $P_a(x_0) = 0$ and x_0 is the only zero of $P_a(x)$, polynomial

$$P_a(x+x_0) = (x+x_0)^{2^l+1} + (x+x_0) + a = x^{2^l+1} + x_0x^{2^l} + x_0^{2^l}x + x$$

has none zeros in $\mathrm{GF}(2^k)^*$. Multiplying the latter polynomial by x_0/x, we obtain that $x_0x^{2^l} + x_0^2x^{2^l-1} + a$ has none zeros in $\mathrm{GF}(2^k)$ and the same can be said about its reciprocal that is equal to $Q(x)$. Thus, all 2^d zeros of $F_a(x)$ are exactly zeros of $Q(x)^{2^l-1}+\Gamma$ and there exists a *unique* $\Delta \in \mathrm{GF}(2^k)^*$ with $\Delta^{2^l-1} = \Gamma^{-1}$ such that $Q(x) = \Delta^{-1}$ has 2^d solutions in $\mathrm{GF}(2^k)$ (note that $Q(x)+b$ has none, one or 2^d zeros depending on $b \in \mathrm{GF}(2^k)$). Also,

$$Q(\Delta) + x_0 = \Delta\left(a\Delta^{2^l-1} + x_0^2\right) = \Delta\left(\frac{x_0^{2^l+1}+x_0}{x_0^{2^l-1}+x_0^{-1}} + x_0^2\right) = 0$$

and, therefore, taking a particular solution v of $Q(x) = \Delta^{-1}$, all the solutions are $v_\mu = v + \mu\Delta$ for every $\mu \in \mathrm{GF}(2^d)$ (these v_μ are exactly the zeros of $F_a(x)$). Now, using $Q(v_\mu) = \Delta^{-1}$, we obtain

$$\begin{aligned}\mathrm{Tr}_k\left(av^{2^l+1} + av_\mu^{2^l+1}\right) &= \mathrm{Tr}_k\left(x_0^2v^2 + x_0v + \Delta^{-1}v + x_0^2v_\mu^2 + x_0v_\mu + \Delta^{-1}v_\mu\right) \\ &= \mathrm{Tr}_k\left(x_0^2\mu^2\Delta^2 + x_0\mu\Delta + \mu\right) = n\mathrm{Tr}_d(\mu)\end{aligned}$$

and if n is odd then

$$\sum_{\mu\in \mathrm{GF}(2^d)} (-1)^{\mathrm{Tr}_k\left(a v_\mu^{2^l+1}\right)} = (-1)^{\mathrm{Tr}_k\left(a v^{2^l+1}\right)} \sum_{\mu\in \mathrm{GF}(2^d)} (-1)^{\mathrm{Tr}_d(\mu)} = 0 \ .$$

This sum can also be calculated directly (see [4, Appendix B]). The case when n is even comes obviously. If $c \neq 1$, we need to multiply all zeros of $F_a(x)$ by c^{-1} to obtain zeros of $F_a(x)$ with $c = 1$. Since $c \in \mathrm{GF}(2^d)$ and $c^{2^l+1} = c^2$, we have the additional coefficient c^{-2} in the trace formulas.

Finally, note that the solution in $\mathrm{GF}(2^k)$ of the equation $y^{2^l} + y = u$ for some $u \in \mathrm{GF}(2^k)$ with $\mathrm{Tr}_d^k(u) = 0$ and odd n can be written in two ways as $\sum_{i=0}^{\frac{n-1}{2}} u^{2^{2il}}$ or $\sum_{i=0}^{\frac{n-3}{2}} u^{2^{(2i+1)l}}$ since $\mathrm{Tr}_d^k(u) = \mathrm{Tr}_l^{nl}(u)$ if $u \in \mathrm{GF}(2^k)$. It can also be calculated directly that if n is odd then $F_a(v_\mu) = 0$ and $\mathrm{Tr}_d^k(v_\mu) = 0$ (see [4, Appendix A]). The identities for $|N_{2^d}|$ follow from Theorem 2. □

Proposition 8 *Take any $a \in \mathrm{GF}(2^k)$. Then polynomial $F_a(x)$ has at least one zero in $\mathrm{GF}(2^k)$. Moreover, if $F_a(x)$ has exactly 2^{2d} zeros then $\mathrm{Tr}_d^k(v) = nc$ for any $v \in \mathrm{GF}(2^k)$ with $F_a(v) = 0$ and, if n is odd, then*

$$\sum_{v\in \mathrm{GF}(2^k),\, F_a(v)=0} (-1)^{\mathrm{Tr}_k\left(ac^{-2}v^{2^l+1}\right)} = 2^d \ .$$

Also if n is odd (resp. n is even) then

$$|N_{2^{2d}}| = \frac{2^{k-d}-1}{2^{2d}-1} \ (\textit{resp.}\ \frac{2^{k-d}-2^d}{2^{2d}-1}) \ .$$

Proof. Since the statement is obvious for $c = 0$, we take $c \neq 0$. As noted above, without loss of generality, we can also assume $c = 1$. Now, select any $u \in \mathrm{GF}(2^k)$ with $\mathrm{Tr}_d^k(u) = 1$ and fix it. Since $\mathrm{Tr}_d^k\left((u+u^2)^{2^l}\right) = 0$, there exists some $w \in \mathrm{GF}(2^k)$ such that $w + w^{2^l} = (u+u^2)^{2^l}$ (see explanations in the proof of Proposition 1). Fix some w with this property as well.

For any pair $(a, v) \in \mathrm{GF}(2^k)\times\mathrm{GF}(2^k)$ with $F_a(v) = 0$ and $v \neq u$, assuming $b = \frac{av^{2^l+1}+w}{(v+u)^{2^l+1}}$, we have

$$\begin{aligned} F_b(v+u) &= \frac{a^{2^l}v^{2^{2l}+2^l} + w^{2^l}}{(v+u)^{2^l}} + (v+u)^{2^l} + \frac{av^{2^l+1}+w}{(v+u)^{2^l}} + 1 \\ &= \frac{1}{(v+u)^{2^l}}\left(v^{2^l}(a^{2^l}v^{2^{2l}} + v^{2^l} + av + 1) + w + w^{2^l} + (u+u^2)^{2^l}\right) = 0 \ . \end{aligned}$$

By Lemma 5, we obtain a 1-to-1 correspondence between two sets

$$\begin{aligned} S_0 &= \{(a,v) \mid v \neq u, F_a(v) = 0, \mathrm{Tr}_d^k(v) = 0\} \quad \text{and} \\ S_1 &= \{(a,v) \mid v \neq u, F_a(v) = 0, \mathrm{Tr}_d^k(v) = 1\} \end{aligned}$$

defined by $(a,v) \mapsto (b, v+u)$ and thus, $|S_0| = |S_1|$. Note that for n odd we can take $u = 1$ and $w = 0$.

Consider equation $F_x(u) = x^{2^l}u^{2^{2l}} + xu + u^{2^l} + 1 = 0$ of the unknown $x \in \mathrm{GF}(2^k)$. After substituting $x = (uu^{2^l})^{-1}y$ we obtain equivalent equation $y^{2^l} + y = (u+u^2)^{2^l}$ which has a solution in $\mathrm{GF}(2^k)$ since $\mathrm{Tr}_d^k\left((u+u^2)^{2^l}\right) = 0$. Thus, $F_x(u) = 0$ has exactly 2^d roots in $\mathrm{GF}(2^k)$ since its linearized homogeneous part $x^{2^l}u^{2^{2l}} + xu$ has 2^d zeros which are $\mu u^{-(2^l+1)}$ for every $\mu \in \mathrm{GF}(2^d)$.

Now, since $F_a(x)$ can have 0, 1, 2^d or 2^{2d} zeros, using Propositions 6 and 7 and Lemma 5, we can compute the following sum in two different ways

$$\begin{aligned} \sum_{(a,v):\, F_a(v)=0} (-1)^{\mathrm{Tr}_d^k(v)} &= |S_0| - |S_1| - 2^d \\ &= (-1)^{\mathrm{Tr}_d^k(1)} + \sum_{a \in N_1} (-1)^{\mathrm{Tr}_d^k(\mathcal{V}_a)} + \sum_{a \in N_{2^d}} \sum_{v:\, F_a(v)=0} (-1)^{\mathrm{Tr}_d^k(v)} + X \\ &= (-1)^n \left(1 + |N_1| - 2^d |N_{2^d}|\right) + X = -2^d \ , \end{aligned}$$

where $X = \sum_{a \in N_{2^{2d}}} \sum_{v:\, F_a(v)=0} (-1)^{\mathrm{Tr}_d^k(v)}$. Thus, if n is odd (resp. n is even) then $X = -\frac{2^{2d}(2^{k-d}-1)}{2^{2d}-1}$ (resp. $\frac{2^{2d}(2^{k-d}-2^d)}{2^{2d}-1}$) (note that $k = nd \geq 2d$ if n is even). Observe that the calculated values of X satisfy

$$X = (-1)^n 2^{2d}(|\mathrm{GF}(2^k)^*| - |N_1| - |N_{2^d}|)$$

which, by Lemma 5, holds if and only only if $\mathrm{Tr}_d^k(v) = n$ and $|N_{2^{2d}}| = \frac{2^{k-d}-1}{2^{2d}-1}$ (resp. $\frac{2^{k-d}-2^d}{2^{2d}-1}$) for any $v \in \mathrm{GF}(2^k)$ with $F_a(v) = 0$ and $a \in N_{2^{2d}}$ if n is odd (resp. n is even). Since $|N_1| + |N_{2^d}| + |N_{2^{2d}}| = |\mathrm{GF}(2^k)^*|$ and $F_0(x)$ has a unique zero $x = 1$, polynomial $F_a(x)$ has at least one zero in $\mathrm{GF}(2^k)$ for any $a \in \mathrm{GF}(2^k)$. Finally, note that zeros of $F_a(x)$ with an arbitrary $c \in \mathrm{GF}(2^d)$ are exactly the elements cv obtained from every $v \in \mathrm{GF}(2^k)$ satisfying $F_a(v) = 0$ with $c = 1$ (obviously, $\mathrm{Tr}_d^k(cv) = nc$).

Now assume n is odd and $c = 1$. To prove the properties of $\mathrm{Tr}_k\left(ac^{-2}v^{2^l+1}\right)$, where $F_a(v) = 0$, we proceed similarly to what we did in the proof of Proposition 7. If $F_a(x)$ has 2^{2d} zeros then, by Theorem 2, $P_a(x)$ has 2^d+1 zeros and

we take one of them, namely, $x_0 \in \mathrm{GF}(2^k)$ with $x_0^{2^l+1}+x_0 = a$. Define polynomial $Q(x) = ax^{2^l}+x_0^2x+x_0$ and denote $\Gamma = x_0^{2^l-1}+x_0^{-1}$ (obviously $\Gamma \neq 0$ since $x_0 \neq 1$). As in Proposition 7, we can write $F_a(x) = Q(x)\left(Q(x)^{2^l-1}+\Gamma\right)$.

Since $P_a(x_0) = 0$ and x_0 is one of 2^d+1 zeros of $P_a(x)$, polynomial

$$P_a(x+x_0) = (x+x_0)^{2^l+1} + (x+x_0) + a = x^{2^l+1} + x_0x^{2^l} + x_0^{2^l}x + x$$

has 2^d zeros in $\mathrm{GF}(2^k)^*$. Multiplying the latter polynomial by x_0/x, we obtain that $x_0x^{2^l} + x_0^2x^{2^l-1} + a$ has 2^d zeros in $\mathrm{GF}(2^k)$ and the same can be said about its reciprocal that is equal to $Q(x)$. Thus, 2^d zeros of $F_a(x)$ are also zeros of $Q(x)$ and the remaining $2^d(2^d-1)$ zeros of $F_a(x)$ are also zeros of $Q(x)^{2^l-1}+\Gamma$. We conclude that for every $\Delta \in \mathrm{GF}(2^k)^*$ with $\Delta^{2^l-1} = \Gamma^{-1}$ (there are 2^d-1 of such Δ) we can find 2^d solutions of $Q(x) = \Delta^{-1}$ in $\mathrm{GF}(2^k)$ (note that $Q(x)+b$ has none, one or 2^d zeros depending on $b \in \mathrm{GF}(2^k)$).

For any $v \in \mathrm{GF}(2^k)$ with $Q(v) = 0$ we have $\mathrm{Tr}_k\left(av^{2^l+1}\right) = \mathrm{Tr}_k\left(x_0^2v^2 + x_0v\right) = 0$. Exactly in the same way as in Proposition 7, we obtain that for odd n,

$$\sum_{v\in\mathrm{GF}(2^k),\, Q(v)=\Delta^{-1}} (-1)^{\mathrm{Tr}_k\left(av^{2^l+1}\right)} = 0$$

for any $\Delta \in \mathrm{GF}(2^k)^*$ with $\Delta^{2^l-1} = \Gamma^{-1}$. In the general case when $c \neq 1$ we need to multiply additionally the trace expression by c^{-2}. □

Therefore, it can be concluded that polynomial $F_a(x)$ has exactly 2^{2d} zeros in $\mathrm{GF}(2^k)$ if and only if $C_n(a) = 0$.

6. Related Linearized Polynomial

In this section, we consider zeros in $\mathrm{GF}(2^{2k})$ of the linearized polynomial

$$Q_a(x) = r^{2^l}a^{2^l}x^{2^{2l}} + x^{2^{k+l}} + rax \ , \tag{29}$$

where $l < k$, $a \in \mathrm{GF}(2^k)^*$ and $r \in \mathrm{GF}(2^{2k})^*$ with $r^{2^k+1} = 1$. For the details on linearized polynomials in general, the reader is referred to Lidl and Niederreiter [12]. It is clear that $Q_a(x)$ does not have multiple roots if $a \neq 0$ and that $Q_a(x)$ always has at least one zero $x = 0$.

Denote $d = \gcd(l,k)$, $n = k/d$ and $d_1 = \gcd(k+l, 2k)$. Observe that

$$Q_a(x) = (r^{-1}a)^{2^{k+l}}x^{2^{2(k+l)}} + x^{2^{k+l}} + rax$$

and in this form, polynomial $Q_a(x)$ reminds $L_a(x)$ defined in (20). For any $u \in \mathrm{GF}(2^k)$ denote $u_i = u^{2^{il}}$ and let $r_i = r^{2^{il}}$ for $i = 0, \ldots, n-1$ so $Q_a(x) = r_1 a_1 x^{2^{2l}} + x^{2^{k+l}} + r_0 a_0 x$. Note that $r^{2^{nl}} = r^{2^{kl/d}} = r^{(-1)^{l/d}}$. Dividing $Q_a(x)$ by $r_0 a_0 a_1^2 x$ (we remove one zero $x = 0$) and using the substitution $y = (ra)^{-1} x^{2^{k+l}-1}$ we obtain

$$f(y) = y^{2^{k+l}+1} + a_1^{-2} y + a_1^{-2} \ , \tag{30}$$

the polynomial that appeared in Theorem 2. Note that multiplying $f(y)$ by $a_0^2 a_1^2$ and using the substitution $z = a^2 y$ we obtain $z^{2^{k+l}+1} + z + a^2$, the polynomial having the same number of zeros as $f(y)$ and that can be analyzed using the results from Sections 3 and 4.

Lemma 6 *Take any $r \in \mathrm{GF}(2^{2k})^*$ with $r^{2^k+1} = 1$. Then r is always a $(2^{k+l}-1)$-th power in $\mathrm{GF}(2^{2k})$ unless $(k+l)/d$ is even and $r^{\frac{2^k+1}{2^d+1}} \neq 1$.*

Proof. Note that $(k+l)/d$ is even if and only if both n and l/d are odd which is equivalent to $d_1 = 2d$. In all other cases, $d_1 = d$. Let ξ be a primitive element of $\mathrm{GF}(2^{2k})$. Then $r = \xi^{(2^k-1)i}$ for some $i \in \{1, \ldots, 2^k+1\}$ and r is a $(2^{k+l}-1)$-th power in $\mathrm{GF}(2^{2k})$ if and only if there exists some $j \in \{1, \ldots, \frac{2^{2k}-1}{2^{d_1}-1}\}$ with $r = \xi^{(2^{d_1}-1)j}$ since $\gcd(2^{k+l}-1, 2^{2k}-1) = 2^{d_1}-1$. Now note that if $d_1 = d$ then for any $i \in \{1, \ldots, 2^k+1\}$ there exists some j with $(2^k-1)i \equiv (2^{d_1}-1)j \pmod{2^{2k}-1}$ since $\gcd(2^{d_1}-1, 2^{2k}-1) = 2^d-1$ divides (2^k-1). If $d_1 = 2d$ then the above equivalence is solvable for j if and only if $\gcd(2^{d_1}-1, 2^{2k}-1) = 2^{2d}-1$ divides $(2^k-1)i$. The latter holds if and only if 2^d+1 divides i since $\gcd(2^d+1, 2^k-1) = 1$. Thus $r = \xi^{(2^k-1)(2^d+1)t}$ for some $t \in \{1, \ldots, \frac{2^k+1}{2^d+1}\}$ which is equivalent to $r^{\frac{2^k+1}{2^d+1}} = 1$. □

Proposition 9 *For any $a \in \mathrm{GF}(2^k)^*$, take polynomials $Q_a(x)$ and $f(y)$ over $\mathrm{GF}(2^{2k})$ defined in (29) and (30) respectively. If $(k+l)/d$ is even and $r^{\frac{2^k+1}{2^d+1}} = 1$ then exactly one of the following holds*

(i) *$f(y)$ has one zero in $\mathrm{GF}(2^{2k})$ and $Q_a(x)$ has 2^{2d} zeros in $\mathrm{GF}(2^{2k})$;*
(ii) *$f(y)$ has two zeros in $\mathrm{GF}(2^{2k})$ and $Q_a(x)$ has one zero in $\mathrm{GF}(2^{2k})$;*
(iii) *$f(y)$ has $2^{2d}+1$ zeros in $\mathrm{GF}(2^{2k})$ and $Q_a(x)$ has 2^{4d} zeros in $\mathrm{GF}(2^{2k})$;*

If $(k+l)/d$ is odd then either

(i) $f(y)$ *has* 2^d+1 *zeros in* $\mathrm{GF}(2^{2k})$ *and* $Q_a(x)$ *has* 2^{2d} *zeros in* $\mathrm{GF}(2^{2k})$ *or;*

(ii) $f(y)$ *has none or two zeros in* $\mathrm{GF}(2^{2k})$ *and* $Q_a(x)$ *has one zero in* $\mathrm{GF}(2^{2k})$.

PROOF. Recall that $f(y)$ is obtained from $Q_a(x)/x$ using the substitution $y=(ra)^{-1}x^{2^{k+l}-1}$ (there is also the multiplicative constant that does not affect the number of zeros). By Theorem 2, $f(y)$ has 0, 1, 2 or $2^{d_1}+1$ zeros in $\mathrm{GF}(2^{2k})$. Since raising elements of $\mathrm{GF}(2^{2k})$ to the power of $(2^{k+l}-1)$ is a $(2^{d_1}-1)$-to-1 mapping, polynomial $Q_a(x)$ can not have more than 2^{2d_1} zeros in $\mathrm{GF}(2^{2k})$. Also, since zeros of $Q_a(x)$ in $\mathrm{GF}(2^{2k})$ form a vector space over $\mathrm{GF}(2^{d_1})$ then $Q_a(x)$ has 1, 2^{d_1} or 2^{2d_1} zeros in $\mathrm{GF}(2^{2k})$. Note that $d_1=d$ unless $(k+l)/d$ is even which gives $d_1=2d$.

Assume $(k+l)/d$ is even and $Z_n(a)\neq 0$ where $Z_n(x)$ comes from (7) (note that $2k/d_1=n$). In this case,

$$\mathrm{N}_{d_1}^{2k}(a)=\mathrm{N}_{2d}^{2k}(a)=\mathrm{N}_{d}^{k}(a)\in\mathrm{GF}(2^d)$$

since $\gcd(2d,k)=d$, and $\mathrm{Tr}_{d_1}\left(\mathrm{N}_{d_1}^{2k}(a)/Z_n^2(a)\right)=0$ since $Z_n(a)\in\mathrm{GF}(2^d)$. Therefore, by Propositions 2 and 3, $f(y)$ always has a zero in $\mathrm{GF}(2^{2k})$.

Now assume $f(y)$ has exactly one zero in $\mathrm{GF}(2^{2k})$ when $(k+l)/d$ is odd (note that $d_1=d$). By Theorem 2, this is equivalent to

$$G(y)=ya_1f\left(a_1^{-1}y^{2^{k+l}-1}\right)=a_2^{-1}y^{2^{2(k+l)}}+a_1^{-2}y^{2^{k+l}}+a_1^{-1}y$$

having 2^d zeros in $\mathrm{GF}(2^{2k})$. Then there exists some $\mathcal{V}\in\mathrm{GF}(2^{2k})^*$ with $G(\mathcal{V})=0$ and all zeros of $G(y)$ are exactly $\{\mu\mathcal{V}\mid\mu\in\mathrm{GF}(2^d)\}$. Note that $G(\mathcal{V}^{2^k})=G(\mathcal{V})^{2^k}=0$ since $a\in\mathrm{GF}(2^k)$ and, thus, $\mathcal{V}^{2^k-1}\in\mathrm{GF}(2^d)$. Take ξ being a primitive element of $\mathrm{GF}(2^{2k})$ and assume $\mathcal{V}=\xi^i$. Then $\mathcal{V}^{2^k-1}\in\mathrm{GF}(2^d)$ if and only if $2^{2k}-1$ divides $i(2^k-1)(2^d-1)$ which is equivalent to 2^k+1 divide $i(2^d-1)$ and, further, to 2^k+1 divide i since $\gcd(2^k+1,2^d-1)=1$. Therefore, $\mathcal{V}\in\mathrm{GF}(2^k)^*$ and $\mathrm{Tr}_d^{2k}\left(a_1\mathcal{V}^{-(2^{k+l}+1)}\right)=0$ which contradicts to the trace condition from Theorem 2 (ii). Thus, $f(y)$ can not have exactly one zero in $\mathrm{GF}(2^{2k})$ under these conditions.

Assume $f(y)$ has exactly one or $2^{d_1}+1$ zeros in $\mathrm{GF}(2^{2k})$ and u is one of them. Then, by Theorem 2, there exists some $v\in\mathrm{GF}(2^{2k})$ with $u=a_1^{-1}v^{2^{k+l}-1}$ and the corresponding $g(v)=0$. In this case, equation $u=(ra)^{-1}x^{2^{k+l}-1}$ is solvable for x if and only if r is a $(2^{k+l}-1)$-th power in

$\mathrm{GF}(2^{2k})$, every solution is a zero of $Q_a(x)$ and all zeros are obtained this way from some u. Thus, by Lemma 6, $Q_a(x)/x$ has respectively $2^{d_1}-1$ or $2^{2d_1}-1$ zeros in $\mathrm{GF}(2^{2k})$ unless $(k+l)/d$ is even and $r^{\frac{2^k+1}{2^d+1}} \neq 1$. In the remaining case, $Q_a(x)/x$ has none zeros in $\mathrm{GF}(2^{2k})$. This also means that in this case, $Q_a(x)$ can not have 2^{2d_1} zeros in $\mathrm{GF}(2^{2k})$ since this leads to $f(y)$ having $2^{d_1}+1$ zeros.

Assume $f(y)$ has exactly two zeros in $\mathrm{GF}(2^{2k})$ (let u is one of them) and consider the cases when r is a $(2^{k+l}-1)$-th power in $\mathrm{GF}(2^{2k})$. Then, by Theorem 2 (i), $ua_1 = x^{2^{k+l}-1}$ is not solvable for x in $\mathrm{GF}(2^{2k})$. Therefore, $ura = ua_1a^{-2^{k+l}+1}r$ is not a $(2^{k+l}-1)$-th power in $\mathrm{GF}(2^{2k})$ and $Q_a(x)/x$ has none zeros in $\mathrm{GF}(2^{2k})$. □

If $(k+l)/d$ is even and $r^{\frac{2^k+1}{2^d+1}} \neq 1$ then

(i) $f(y)$ has one or $2^{2d}+1$ zeros in $\mathrm{GF}(2^{2k})$ and $Q_a(x)$ has one zero in $\mathrm{GF}(2^{2k})$;

(ii) $f(y)$ has two zeros in $\mathrm{GF}(2^{2k})$, $Y_n(a) \neq 0$ and $Q_a(x)$ has one zero in $\mathrm{GF}(2^{2k})$;

(iii) $f(y)$ has two zeros in $\mathrm{GF}(2^{2k})$, $Y_n(a) = 0$ and $Q_a(x)$ has 2^{2d} zeros in $\mathrm{GF}(2^{2k})$.

Note that if $(k+l)/d$ is even, $r^{\frac{2^k+1}{2^d+1}} \neq 1$ and $Z_n(a) = 0$ (the latter, by Note 1 and Propositions 4 and 5, is equivalent to $f(y)$ having 1 or $2^{d_1}+1$ zeros) then $Q_a(x)$ has one zero in $\mathrm{GF}(2^{2k})$ (observe that $2k/d_1 = n$).

For $0 < j \leq i$ and $u \in \mathrm{GF}(2^k)$, let $D_u^{j,i}$ denote a three-diagonal matrix of size $i-j+2$ that contains ones on the main diagonal and with

$$D_u^{j,i}(t,t+1) = r_{j+t}^{(-1)^{j+t-1}} u_{j+t} \quad \text{and} \quad D_u^{j,i}(t+1,t) = r_{j+t}^{(-1)^{j+t}} u_{j+t}$$

for $t = 0, \ldots, i-j$, where indices of u are reduced modulo n, indices of r are reduced using the rule $r_{tn+i} = r_i^{(-1)^{tl/d}}$ ($i = 0, \ldots, n-1$ and $t \geq 0$), rows and columns of $D_u^{j,i}$ are numbered from 0 to $i-j+1$. The determinant of $D_u^{j,i}$, denoted as $\Delta'_u(j,i)$, can be computed expanding by minors along the last row to obtain

$$\Delta'_u(j,i) = \Delta'_u(j,i-1) + u_i^2 \Delta'_u(j,i-2)$$

assuming $\Delta'_u(j,i) = 1$ if $i-j \in \{-2,-1\}$. Comparing the latter recursive identity with (11) it is easy to see that

$$\Delta'_u(j,i) = \Delta_u(j,i) \ . \tag{31}$$

Proposition 10 *Let $(k+l)/d$ be even and take any $a \in \mathrm{GF}(2^k)^*$. Then $Q_a(x) = 0$ has exactly one root in $\mathrm{GF}(2^{2k})$ that is equal to zero if $Z_n^2(a) \neq \mathrm{N}_d^k(a)(\delta+\delta^{-1})$, where $\delta = r^{\frac{2^k+1}{2^d+1}} \in \mathrm{GF}(2^{2d})$ is a (2^d+1)-th root of unity over $\mathrm{GF}(2)$ and $Z_n(x)$ comes from (7).*

Proof. Note that $\delta + \delta^{-1} \in \mathrm{GF}(2^d)$ and thus, $Y_n(u) \in \mathrm{GF}(2^d)$ for any $u \in \mathrm{GF}(2^k)$ since $Z_n(u) \in \mathrm{GF}(2^d)$.

Obviously, $Q_a(0) = 0$ and we have to show that this is the only zero of $Q_a(x)$ in $\mathrm{GF}(2^{2k})$ if $Y_n(a) \neq 0$. Taking equation $Q_a(x) = 0$ and all its 2^{2li} powers we obtain n equations

$$Q_a^{2^{2il}}(x) = x^{2^{(2i+1)l+k}} + r_{2i+1}a_{2i+1}x^{2^{2l(i+1)}} + r_{2i}a_{2i}x^{2^{2li}} = 0 \quad \text{for} \quad i = 0, \ldots, n-1 \ ,$$

where indices of a are reduced modulo n and indices of r are reduced using the rule $r_{tn+i} = r_i^{(-1)^{tl/d}}$ ($i = 0, \ldots, n-1$ and $t \geq 0$). If x_{2i} ($i = 0, \ldots, n-1$) are considered as independent variables then matrix $\mathcal{M}_n$ of the obtained system of n linear equations with n unknowns consists of three cyclic antidiagonals and

$$\begin{aligned} \mathcal{M}_n(i, (n-3)/2 - i) &= 1 \ , \\ \mathcal{M}_n(i, n-i-1) &= r_{2i}a_{2i} \ , \\ \mathcal{M}_n(i, n-i-2) &= r_{2i+1}a_{2i+1} \quad \text{for} \quad i = 0, \ldots, n-1 \ , \end{aligned}$$

where rows and columns of $\mathcal{M}_n(i,j)$ are numbered from 0 to $n-1$ and all elements of $\mathcal{M}_n$ are indexed modulo n.

Now permute the columns and rows of $\mathcal{M}_n$ in the following way. Decimate the rows as $i(n+1)/2$ and columns as $(n-3)/2 + i(n-1)/2$ modulo n for $i = 0, \ldots, n-1$ (note that $\gcd((n+1)/2, n) = \gcd((n-1)/2, n) = 1$). Then the obtained matrix $\mathcal{M}'_n$ is three-diagonal cyclic with

$$\begin{aligned} \mathcal{M}'_n(i,i) &= \mathcal{M}_n(i(n+1)/2, (n-3)/2 + i(n-1)/2) = 1 \ , \\ \mathcal{M}'_n(i,i-1) &= \mathcal{M}_n(i(n+1)/2, (n-3)/2 + (i-1)(n-1)/2) = r_{i(n+1)}a_{i(n+1)} \ , \\ \mathcal{M}'_n(i,i+1) &= \mathcal{M}_n(i(n+1)/2, (n-3)/2 + (i+1)(n-1)/2) = r_{i(n+1)+1}a_{i(n+1)+1} \end{aligned}$$

for $i = 0, \ldots, n-1$ (indices of r and a are calculated modulo $2n$) since

$$\begin{aligned} i(n+1)/2 + (n-3)/2 + i(n-1)/2 &= (n-3)/2 + in \equiv (n-3)/2 \pmod{n} \ , \\ i(n+1)/2 + (n-3)/2 + (i-1)(n-1)/2 &= -1 + in \equiv n-1 \pmod{n} \ , \\ i(n+1)/2 + (n-3)/2 + (i+1)(n-1)/2 &= n-2+in \equiv n-2 \pmod{n} \ . \end{aligned}$$

Also note that $a_{i(n+1)} = a_i$ since $a \in \mathrm{GF}(2^{nk})$ and $r_{i(n+1)} = r_i^{(-1)^i}$ since $r_{n+i} = r_n^{2^{ik}} = r_i^{-1}$ for any $i \geq 0$. Then for $i = 0, \ldots, n-1$

$$\mathcal{M}'_n(i, i+1) = r_{i+1}^{(-1)^i} a_{i+1} \quad \text{and} \quad \mathcal{M}'_n(i+1, i) = r_{i+1}^{(-1)^{i+1}} a_{i+1} \quad \text{so}$$

$$\mathcal{M}'_n = \begin{pmatrix} 1 & r_1 a_1 & 0 & \cdots & r_0 a_0 \\ r_1^{-1} a_1 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & & \ddots & 1 & r_{n-1}^{-1} a_{n-1} \\ r_0^{-1} a_0 & 0 & \cdots & r_{n-1} a_{n-1} & 1 \end{pmatrix} .$$

Note that a principal submatrix obtained by deleting the last column and the last row from $\mathcal{M}'_n$ is exactly $D_a^{1,n-2}$.

We also have to apply the decimation $(n-3)/2 + i(n-1)/2$ modulo n for $i = 0, \ldots, n-1$ (used to permute the columns of $\mathcal{M}$) to the vector of unknowns $(z_{2(n-1)}, z_{2(n-2)}, \ldots, z_2, z_0)$. This results in $\boldsymbol{z} = (z_{n+1}, z_2, z_{n+3}, \ldots, z_{n-1}, z_0)^{\mathrm{T}}$, where the increment for the index of z is equal to $n-1$ starting from 0 and going right to left (indices are calculated modulo $2n$). Now, if $\mathbf{0} = (0, \ldots, 0)^{\mathrm{T}}$ then a new system has the following matrix representation

$$\mathcal{M}'_n \boldsymbol{z} = \mathbf{0} \ . \tag{32}$$

The determinant of $\mathcal{M}_n$ is equal to the determinant of $\mathcal{M}'_n$ and can be computed expanding the latter by minors along the last row. Doing this it is easy to see that

$$\begin{aligned} \det \mathcal{M}'_n \quad &= \quad \Delta'_a(1, n-2) + r_{n-1} a_{n-1} \left(r_{n-1}^{-1} a_{n-1} \Delta'_a(1, n-3) + \prod_{i=0}^{n-2} r_i^{(-1)^i} a_i \right) \\ &\qquad + r_0^{-1} a_0 \left(r_0 a_0 \Delta'_a(2, n-2) + \prod_{i=1}^{n-1} r_i^{(-1)^{i-1}} a_i \right) \\ &\overset{(12,13,31)}{=} B_n^2(a) + a_{n-1}^2 B_{n-1}^2(a) + (a_0 B_{n-1}^{2^k}(a))^2 + \mathrm{N}_k^{nk}(a)(\delta + \delta^{-1}) \\ &\overset{(4,7)}{=} Z_n^2(a) + \mathrm{N}_k^{nk}(a)(\delta + \delta^{-1}) = Y_n(a) \ . \end{aligned}$$

Thus, if $Y_n(a) \neq 0$ then (32) has only zero solution. Now note that every $v \in \mathrm{GF}(2^{2nk})$ with $Q_a(v) = 0$ provides a solution to the system given by $v_{2i} = v^{2^{2ik}}$ for $i = 0, \ldots, n-1$. Therefore, if $Y_n(a) \neq 0$ then $Q_a(z)$ has at most one zero. □

7. Conclusion

We studied the polynomials $P_a(x) = x^{2^l+1} + x + a$ over GF(2^k) with $l < k$ and proved some new criteria for the number of zeros of $P_a(x)$ in GF(2^k). In particular, the number of zeros and the trace of the value of the polynomial, due to Dobbertin, in point a^{-1} are related when $\gcd(l, k) = 1$. In case when there is a unique zero or exactly two zeros and $\gcd(l, k)$ is odd, we provided explicit expressions for calculating these roots as polynomials of a. We also found the distribution of the number of zeros of $P_a(x)$. Finally, we studied the affine polynomial $F_a(x) = a^{2^l} x^{2^{2l}} + x^{2^l} + ax + c$ with $c \in \mathrm{GF}(2^{\gcd(l,k)})$, which was shown to be closely related to $P_a(x)$. In many cases, we were able to provide explicit expressions for calculating zeros of $F_a(x)$.

References

[1] J. F. Dillon, Geometry, codes and difference sets: Exceptional connections, in: Ákos Seress, K. T. Arasu (Eds.), Codes and Designs, Vol. 10 of Ohio State University Mathematical Research Institute Publications, Walter de Gruyter, Berlin, 2002, pp. 73–85.

[2] H. Dobbertin, P. Felke, T. Helleseth, P. Rosendahl, Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums, IEEE Trans. Inf. Theory 52 (2) (2006) 613–627.

[3] T. Helleseth, A. Kholosha, G. J. Ness, Characterization of m-sequences of lengths $2^{2k} - 1$ and $2^k - 1$ with three-valued crosscorrelation, IEEE Trans. Inf. Theory 53 (6) (2007) 2236–2245.

[4] T. Helleseth, A. Kholosha, m-sequences of lengths $2^{2k}-1$ and 2^k-1 with at most four-valued cross correlation, in: S. W. Golomb, M. G. Parker, A. Pott, A. Winterhof (Eds.), Sequences and Their Applications - SETA 2008, Vol. 5203 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2008, pp. 106–120.

[5] A. W. Bluher, On $x^{q+1} + ax + b$, Finite Fields and Their Applications 10 (3) (2004) 285–305.

[6] R. Lidl, G. L. Mullen, G. Turnwald, Dickson Polynomials, Vol. 65 of Pitman monographs and surveys in pure and applied mathematics, Longman Scientifc and Technical, Harlow, 1993.

[7] J. F. Dillon, H. Dobbertin, New cyclic difference sets with Singer parameters, Finite Fields and Their Applications 10 (3) (2004) 342–389.

[8] T. Helleseth, A. Kholosha, On the equation $x^{2^l+1} + x + a = 0$ over GF(2^k), Finite Fields and Their Applications 14 (1) (2008) 159–176.

[9] H. Dobbertin, Kasami power functions, permutation polynomials and cyclic difference sets, in: A. Pott, P. V. Kumar, T. Helleseth, D. Jungnickel (Eds.), Difference Sets, Sequences and their Correlation Properties, Vol. 542 of NATO Science Series, Series C: Mathematical and Physical Sciences, Kluwer Academic Publishers, Dordrecht, 1999, pp. 133–158.

[10] V. P. Il'in, Y. I. Kuznetsov, Three-Diagonal Matrices and their Applications, Nauka, Moscow, 1985, (in Russian).

[11] T. Helleseth, V. Zinoviev, Codes with the same coset weight distributions as the $\mathbf{Z}_4$-linear Goethals codes, IEEE Trans. Inf. Theory 47 (4) (2001) 1589–1595.

[12] R. Lidl, H. Niederreiter, Finite Fields, Vol. 20 of Encyclopedia of Mathematics and its Applications, Cambridge University Press, Cambridge, 1997.